الجامعة اللبنانية

كلية الحقوق والعلوم السياسية والإدارية

العمادة

العملات التشفيرية: ظاهرة جديدة في الحقل القانوني والجرمي

دراسة مقارنة وتحليل

رسالة أعدّت لنيل شهادة الماستر 2 بحثي في القانون الجزائي

إعداد

ماريلين اورديكيان

لجنة المناقشة

الدكتورة جنان الخوري	الأستاذة المشرفة	رئيسةً
الدكتور رامي عبد الحي	أستاذ	عضواً
الدكتور علي رحال	أستاذ	عضواً

2020



الإهداء

إلى ساتوشي ناكاموتو

الشكر

أشكر والدتي التي ضحت بالكثير ولطالما سهرت لكي أتمكن من تحقيق أهدافي. أشكر رفيق الدرب باليك، الذي يحفزني على المثابرة ويحثني في أخذ خطوات جريئة في الحياة. أتوجه بجزيل الشكر والامتنان إلى صديقتيّ سارا ونور اللتين قضيت معهما الأيام الجميلة والمرة في الكلية.

أتوجه بالشكر والتقدير الفائق للدكتورة جنان الخوري المشرفة على هذه الرسالة... فمهما قلت من ثناء، لن أتمكن من شكرها على مجهودها وعلى نصائحها الغفيرة التي لا تقتصر فقط على فترة تحضير الرسالة.

أشكر أساتذتي في كلية الحقوق وعلى وجه الخصوص الدكتور عصام مبارك الذي كان ولا يزال من أكبر الداعمين الحقيقيين لمسيرتي الأكاديمية، والدكتورة ماري الحلو التي زرعت بداخلي العشق والشغف للقانون الجزائي.

كما أشكر أعضاء لجنة المناقشة المحترمين الدكتور رامي عبد الحي والدكتور علي رحال.

التصميم العام للدراسة:

القسم الأول: الإطار القانوني للعملات التشفيرية

الباب الأول: مفهوم العملات التشفيرية

الفصل الأول: ماهية العملات التشفيرية

الفصل الثاني: الوصف القانوني للوسائل التقنية

الباب الثاني: تَبعة المفاعيل التطبيقية للعملات التشفيرية

الفصل الأول: المخاطر الناتجة عن العملات التشفيرية

الفصل الثاني: التطبيقات القانونية لتنظيم العملات التشفيرية

القسم الثاني: جرائم العملات التشفيرية

الباب الأول: العملات التشفيرية منفذٌ لتمويل الإرهاب

الفصل الأول: مفهوم التمويل السيبراني للإرهاب

الفصل الثاني: في التشريع

الباب الثاني: الجرائم السيبرانية

الفصل الأول: الأفعال المرتكبة عبر البرمجيات الخبيثة

الفصل الثاني: التقليد الرقمي

المقدمة

في السابع عشر من شهر كانون الأول من العام 2017 وصلت قيمة عملة البيتكوين **bitcoin** التشفيرية إلى عتبة العشرين ألف دولار أميركي. من حينه، لم تعد مجرّد عملة رقمية وتقنية مقتصرة على التقنيين والمختصين، بل أسرت اهتمام العالم وجذبت أشهر الشركات العالمية وكبار المستثمرين، والأهم أصبح المواطن العادي الذي لم يسمع بها قط من عداد المتشوقين لاستكشافها. كانت ثورة البيتكوين متوقعة ففي عصر الذكاء الاصطناعي وإنترنت الأشياء والتقنيات الأخرى التي نقلت العالم إلى عصر التكنولوجيا المتقدمة، كانت النقود ولا تزال تعاني من الرجعية بحيث لم تكن تجاري العصر فأتت تقنية البيتكوين **Bitcoin** المبنية على البلوكشاين (سلسلة الكتل) **Blockchain** لتقلب كل المعايير.

تعود جذور العملات الرقمية إلى عالِم التشفير دايفيد شوم **David Chaum** الذي نشر في العام 1983 ورقة علمية بعنوان **Blind Signatures for Untraceable Payments** والتي أوجزت فكرة عملة رقمية مجهولة غير قابلة للتتبع[1]. يُعتبر "شوم" الأب الروحي لحركة **Cypherpunk** الشهيرة التي عملت على برامج تحمي الحركة المجهولة على شبكة الإنترنت والخصوصية الرقمية خصوصاً من الاختراق المحتمل من قبل الدولة ومؤسساتها المعنية[2]، وذلك على غرار مواضيع ترتبط بفكرة عملة رقمية محررة من الخصائص التقليدية. وتكريساً لأفكاره، ابتكر "شوم" في العام 1990 الـ **DigiCash** عاكساً المفهوم الذي أوجزه في بحثه السابق ذكره[3]. تلى مشروع "شوم" في العام 1996 الـ **E-Gold** [4]، وفي العام 1998 ساهم عالِم التشفير واي داي **Wei Dai** من إثارة الاهتمام بالعملات الرقمية مجدداً من خلال نشره لورقة تبحث فكرة **b-money**، وهو نظام نقدي إلكتروني موزّع يعتمد على المجهولية الرقمية **Digital Anonymity**.

---

[1] David Chaum. "Blind signatures for untraceable payments." Advances in cryptology, *Springer*, 1983, pp. 199-203.

[2] Arvind Narayanan. "What Happened to the Crypto Dream?, Part 1," IEEE Security & Privacy, Vol. 11.2, March–April 2013, pp. 75-76.

[3] Waleed Abrar. "Untraceable electronic cash with Digicash," University of Konstanz, Jul. 2014, p. 1, Researchgate.net, Accessed 3 Jan. 2020.

[4] https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/e-gold.html, Accessed 10 Jan. 2020.

إن هذه الورقة في غاية الأهمية لأنها حددت الخصائص الأساسية لجميع أنظمة التشفير **Encryption**[5] المعتمدة في العصر الحديث[6]. أما عن آخر وأبرز التجارب لابتكار عملة رقمية بديلة (قبل البيتكوين)، فكانت تلك التي أصدرها موقع **Liberty Reserve** في العام 2006 الذي قدّم خدمة تحويل عملة رقمية تحمل الاسم عينه[7].

بالرغم من فشل كل هذه المحاولات من إيجاد البديل للنقود الرسمية وذلك لخلفيات عديدة أبرزها تسهيلها ارتكاب جرائم تابعة إلى فئات مختلفة[8]، إلا أنه لا يمكن إنكار دورها في بلورة عملات العصر العملات الرقمية التشفيرية.

"وُلد" البيتكوين في العام 2008 في أعقاب الأزمة المالية والاقتصادية التي أسفرت إلى انهيار شبه كامل للنظام المصرفي[9]... في وقت فُقد وانعدم عنصر الثقة بالمؤسسات المصرفية والمالية، ناهيك عن بداية اكتساح التجارة الإلكترونية آنذاك والتي باتت تهدد وتستبدل وسائل التجارة التقليدية. ففي هذه التجارة وسيلة الدفع هي بشكل شبه حصري معتمدة على المؤسسات المالية التي تعمل كوسيط موثوق به لمعالجة التحاويل والمدفوعات المالية، هذا الأمر منح هذه المؤسسات قوة كبرى بإجراء وتنظيم والتحكم والسيطرة على كل العمليات المالية، بحيث باتت لهم السلطة التقديرية بقبول أو رفض إجراء تحويل، على غرار الفترة الزمنية المطلوبة لإتمام العملية والتكلفة العالية. فأضحت هذه المؤسسات على علم بجميع التحركات المالية لعملائها لدرجة تخطيها حدود الخصوصية الرقمية في الكثير من الأحيان، خصوصاً عن طريق جمع ومعالجة البيانات الخاصة الرقمية.

---

[5] تقنية التشفير/Encryption: آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن ارجاعها إلى حالتها الأصلية. قوام هذه التقنية هي خوارزمية Algorithm رياضية ذكية تسمح لمن يمتلك مفتاحاً سرياً، بأن يحوّل رسالة مقروءة إلى رسالة غير مقروءة والعكس صحيح. أي أنه يتم استخدام المفتاح السري لفك الشيفرة وإعادة الرسالة المشفّرة إلى وضعيتها الأصلية.

–طوني عيسى، **التنظيم القانوني لشبكة الإنترنت دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية**، أطروحة أُعدت لنيل شهادة الدكتوراه، الجامعة اللبنانية كلية الحقوق والعلوم السياسية والإدارية الفرع الثاني، 2000، ص. 382.

[6] Wei Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[7] United States v. Liberty Reserve, 13 Crim. 368 (S.D.N.Y. May 20, 2013), www.archive.org, Accessed 6 Dec. 2019.

[8] Lawrence J. Trautman. "Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?" Richmond Journal of Law and Technology, Vol. 20.4, 2014, pp. 1-108, p. 2.

[9] Michael KF Chui et al. "The collapse of international bank finance during the crisis: evidence from syndicated loan markets." BIS Quarterly Review, Sept. 2010, pp. 39-49, p. 39.

في هذه المرحلة وفي فترة الريبة، كان ظهور البديل أثراً منطقياً... وبالفعل، بتاريخ 31 تشرين الأول من العام 2008 نشر شخص أو جهة مجهولة تُدعى بساتوشي ناكاموتو **Satoshi Nakamoto**، ورقة بيضاء بعنوان "بيتكوين: نظام نقد إلكتروني قائم على النظير للنظير" "**Bitcoin: A Peer-to-Peer Electronic Cash System**"[10] والتي تعتبر العامود الفقري للبيتكوين والعملات التشفيرية اللاحقة المعروفة بالعملات البديلة **Altcoins**.

حرر "ناكاموتو" فكرة "الخدمات المصرفية" من المصارف المركزية، مقدماً لأصحاب المصالح والشركات والمستهلك وسيلة لتنفيذ المعاملات المالية دون الاتكاء على طرف واحد مركزي. عرّف البيتكون بأنه "نقد إلكتروني مبني على النظير للنظير[11] يسمح بإنجاز عملية الدفع الإلكتروني مباشرةً من طرف إلى آخر من دون المرور عبر مؤسسة مالية"، ويضيف "ناكاموتو" بأن النظام اللامركزي هذا يكرّس مبادئ التشفير والتوقيع الإلكتروني عوضاً عن عنصر الثقة، وهو حل لمشكلة الإنفاق المضاعف **Double-Spending** التي تعاني منها وسائل الدفع بالنقد الإلكتروني[12]. فإذاً، يمكن تعريف البيتكوين بأنها عملة رقمية تشفيرية **Cryptocurrency** لا تصدر ولا تسيطر عليها أي دولة أو مصرف مركزي. تُنجز التحويلات من طرف إلى آخر مباشرةً من دون وسيط (كالمصرف)، وتتم عملية تصديق التحويلات على شبكتها عبر العُقد **Nodes** وعبر تكريس مبادئ وتقنيات التشفير بحيث تُسجّل كافة العمليات على السجل العام العلني الموزّع المعروف بالبلوكشاين. أما عن كيفية إصدار عملة بيتكوين جديدة فهي تتم عن طريق عملية تسمى بالتعدين **Mining** [13].

سرعان ما انتشرت عملة البيتكوين والعملات التشفيرية وكثر التعامل بها، فعلى أرض الواقع هناك حوالي 2417 عملة تشفيرية[14]، وبلغت عدد المحفظات الإلكترونية (التي تُحفظ فيها العملات) على البلوكشاين الـ 44 مليون بنهاية عام 2019 في حين كانت قرابة 10 ملايين في الربع الثالث من العام

---

[10] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, www.bitcoin.org.

[11] نظير لنظير Peer to Peer أي من شخص إلى آخر (أو جهة).

[12] Brian Patrick Eha. **How Money Got Free: Bitcoin and the Fight for the Future of Finance**, Oneworld Publications, 2017, p. 12.

[13] سيتم معالجة الموضوع في القسم الأول.

[14] https://coinmarketcap.com/all/views/all/, Accessed 29 Feb. 2020.

2016 [15]، الأمر الذي دفع الكثر بالاعتقاد بأن العملات التشفيرية هي ثورة في عالم الاقتصاد والمال والتكنولوجيا وذلك لقدرتها على تهديد المصارف المركزية التي تحتكر سلطة إصدار النقود[16]. ويرى الدكتور سيف الدين عمّوص بأن البيتكوين يُمثّل حلاً تكنولوجياً جديداً لمشكلة النقد، خصوصاً بأنه يستخدم العديد من الابتكارات التقنية والتكنولوجية التي تم تطويرها على مدى العقود القليلة الماضية، مستفيداً من التجارب العديدة لإنتاج النقد الإلكتروني[17]. فهي توفّر أيضاً السرعة الفائقة في إتمام التحويلات التي تُنجز مقابل رسم بخس، وذلك في بيئة رقمية آمنة ومشفّرة مزوّدة بميزة المجهولية **Anonymity** أو على الأقل بشبه المجهولية (والاسم المستعار) **Pseudonym**.

ولكن مع كل ذلك، تطرح العملات التشفيرية إشكاليات عدة أهمها قانونية، فهي لا تصدر عن جهة رسمية ولا تنظمها القوانين على عكس النقود الرسمية **Fiat Currency** وطبيعتها العالمية والعابرة للحدود تعسّر معضلة احتوائها. وما يزيد من صعوبة إحاطتها ببيئة تشريعية، هي واقعة تخلّف وعدم مجاراة السلطات التشريعية وسلطات إنفاذ القانون التطورات التكنولوجية وعدم اعتمادهم آلية التأقلم وتنظيم هذه الظواهر الحديثة في مراحلها الابتدائية. على غرار ذلك، وبالرغم من محاولات عديدة لتنظيمها قانوناً، يشكّل انعدام الاجماع على طبيعتها وتسميتها العائق الأول أمام المشرعين يلحقه قيام التناقض والاختلاف في النهج التنظيمي والقوانين المطبّقة، الأمر الذي ينعكس سلباً على أي إمكانية للتطور والتقدم. ونتيجة ذلك، ظهرت مقاربات غفيرة كثيرة سنعمد إلى عرضها والإضاءة على ثغراتها مع تبيان الاختلال بين المواقف الدولية والإقليمية والقوانين الوضعية من بينها لبنان، مع الإشارة إلى مدى تعقيد عملية إنفاذ القوانين الوضعية والدولية المعمول بها. إن هذه المواقف في غاية الأهمية لأنها تضع حجر الأساس لآلية التفاعل مع العملات التشفيرية، وبالأخص التعامل مع الأفعال غير المشروعة والجرائم المقترفة بواسطتها أو عليها.

إن انعدام السيطرة والرقابة الرسمية على العملات التشفيرية وإطاحة الوسطاء مجتمعةً مع ميزات تقنية مثل إخفاء الهوية الرقمية، تسمح باستغلالها كأداة لإجراء المعاملات دون إشراف رسمي، لا بل يمكن الوصول إليها بسهولة من قبل المجرمين سواء السيبرانيين أو مرتكبي الجرائم المنظمة والاقتصادية أو

---

[15] https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/, Accessed 29 Feb. 2020.

[16] Grégory Claeys, et al. Study requested by the European Parliament's Economic and Monetary Affairs Committee (ECON), on "**Cryptocurrencies and Monetary Policy**," No. PE 619.018, Jun. 2018, p. 6.

[17] د. سيف الدّين عمّوص، **معيار البيتكوين البديل اللامركزي للنظام المصرفي المركزي**، ترجمة محمد أحمد حمدان، الطبعة الأولى، تموز 2019، ص. 192.

الجرائم العادية. يشير عدد من التحقيقات والاجتهادات البارزة واتجاهات فقهية إلى أن عملة البيتكوين وسائر العملات التشفيرية أصبحت العملة المفضلة للعديد من المجرمين[18] بحيث تخطت قيمة الأموال المستقبلة من قبل هؤلاء الـ 12 مليار دولار أميركي في العام 2019[19]. فتبلورت أفعال جديدة معقدة بطبيعتها مثل التعدين غير المشروع، وانتشرت أسواق سوداء في الجانب المظلم من شبكة الإنترنت **Dark Web**... أسواق تبيع خدمات غير مشروعة وممنوعات كالأسلحة والمخدرات وبيع بيانات شخصية وتعيين قاتلين مستأجرين والإتجار بالأشخاص إلخ. كلها متاحة للبيع مقابل عملات تشفيرية من دون رقيب! ومع ارتفاع قيمتها، انحازت الجرائم السيبرانية والمجرم السيبراني نحو هذه العملات، فأصبحت في الوقت عينه أولاً، الهدف بحيث تتمثل مدفوعات الضحايا على شبكة الإنترنت بها وثانياً، تسهّل عمليات الإنفاق وتحويل الأموال فيما بين المجرمين وثالثاً، هي وسيلة لتخبئة محاصيلهم الجرمية. أما النصيب الأكبر يعود إلى الجرائم المنظمة والاقتصادية والعادية مثل تبييض الأموال وتمويل الإرهاب على غرار السرقة وعمليات الاحتيال الإلكترونية التي أخذت طابعاً حديثاً بدخول عنصر العملات التشفيرية، علماً أن لبنان ليس غريباً عن هذه الأحداث[20] خصوصاً بعد لجوء الكثر إلى عملة البيتكوين كبديل بعد تدهور الوضع الاقتصادي وزيادة القيود المصرفية على العملاء في الربع الأخير من العام 2019[21].

استدراكاً لخطورة الوضع، بادرت دول عديدة ومنظمات وجهات دولية بوضع بيئة تشريعية تتطرّق وتشمل العملات التشفيرية والأفعال الجرمية المرتكبة بواسطتها أو التي تستهدفها، وذلك كمحاولة للحد من مفاعليها ومخاطرها خصوصاً بعد ظهور مشكلة مدى ملاءمة القوانين الحالية في مواجهتها. تم إرساء نماذج متنوعة، فالبعض اختار المنع أو التحذير من هذه العملات، في حين عمدت جهات أخرى على تنظيمها وتشريعها، كيف؟ عبر سن قوانين جديدة خاصة بها أو عبر تعديل قوانين وأنظمة قائمة أصلاً.

---

[18] Steven David Brown. "Cryptocurrency and Criminality: The Bitcoin Opportunity." The Police Journal, Vol. 89.4, Dec. 2016, pp. 327–339, p. 327.

[19] Chainalysis. Report on **The 2020 State of Crypto Crime**, January 2020, p. 5, www.chainalysis.com, Accessed 2 Feb. 2020.

[20] بعد أن كثرت عمليات التهديد والاحتيال الإلكتروني سواء عبر الرسائل النصية أو البريد الإلكتروني، حذّرت قوى الأمن الداخلي عبر مواقع التواصل الاجتماعي من هذه العمليات التي تدفع بالمواطنين إلى ارسال قيمة معينة من عملة البيتكوين إلى المقرصنين.

– راجع الملحق رقم 3، موضوعه التحذير المذكور والذي تم نشره بتاريخ 18 نيسان من العام 2020.

[21] Timour Azhari. "Distrust in Lebanese banks spurs bitcoin boom." Al Jazeera, 25 Feb. 2020, www.aljazeera.com, Accessed 27 Feb. 2020.

–أيضاً:

–Maher Nadeem. "Some see Bitcoin as haven in crisis-hit Lebanon." The Daily Star, 31 Jan. 2020, www.dailystar.com.lb, Accessed 2 Feb. 2020.

من أبرز وأول المبادرات الدولية نذكر تلك التي أقدمت عليها مجموعة العمل المالي **FATF** [22] التي عمدت إلى إصدار تقارير ودراسات مفصلة بشكل دوري، لحين تعديل توصياتها لتشملها. خطا الاتحاد الأوروبي على خُطى مجموعة العمل المالي بحيث عدّل أهم قانون إقليمي يُعنى بتبييض الأموال وتمويل الإرهاب الـ **AMLD 5** [23] ليشمل هذه العملات. إلا أن هذه المبادرات على غرار العديد من غيرها اقتصرت على أفعال معدودة وغير شاملة لكافة الجرائم، تتمثل في هذه الحالة بتبييض الأموال وتمويل الإرهاب.

وعليه، تكمن أهمية الدراسة بأنها ستعالج العملات التشفيرية من الناحية القانونية وخصيصاً من منظار عالم الجريمة. فلقد عمدنا إلى مناقشة موضوع ذات الصعوبة والتعقيدات التقنية بلغة بسيطة وذات المقاربة القانونية، بحيث من ليست له أي خلفية تقنية يتمكّن من فهم الإشكاليات التي تطرحها هذه الثورة المالية والتكنولوجية التي اكتسحت العالم، فعالجنا هذه الإشكاليات الكثيرة واحدة تلو الأخرى ممهدين إلى الأقسام والمسائل القانونية اللاحقة الأكثر تعقيداً. على غرار ذلك، إن بموجب هذه الدراسة طرحنا وناقشنا لأول مرة[24] العملات التشفيرية في لبنان انطلاقاً من قانون المعاملات الإلكترونية وذات الطابع الشخصي[25]، فعرضنا أخطاء وثغرات وقع بها المشرّع اللبناني بعضها يجعل نصوصها غير قابلة للتطبيق سواء لاستحالة تقنية أو لتعارضها مع قانون العقوبات اللبناني. أما من الناحية الدولية، ونظراً للتحديث الدائم وحصول تعديلات وسنّ قوانين جديدة ترعى العملات التشفيرية على مدار متتابع، فإنه بموجب هذه الرسالة تسنّا لنا أن نكون من أول الباحثين والمناقشين لبعضٍ من أجدد النصوص القانونية خصوصاً تلك الصادرة عن مجموعة العمل المالي والاتحاد الأوروبي، بحيث عرضناها وبيّنا بعضاً من العوائق والصعوبات التي تطرحها. ويبقى هدفنا الأكبر إزالة الغموض عن مفهوم البيتكوين والعملات التشفيرية لإثبات أنها وبالرغم من منافعها العديدة، تشكل خطراً كبيراً ومحدقاً فيما يتعلق بعالم الجريمة.

ولما كانت هناك إشكاليات قانونية وموضوعية وإجرائية تبرز على الصُعد الدولي والإقليمي والمحلي في مجالات مختلفة ولكن مترابطة (بشكل وثيق)، سواء على صعيد قانون العقوبات وقوانين مكافحة الجرائم السيبرانية والقوانين المصرفية والنقدية، لا سيما في لبنان خصوصاً عندما نتواجه مع مبدأ شرعية الجرائم

---

[22] Financial Action Task Force

[23] Fifth Anti-Money Laundering Directive

[24] بالإضافة الى دراسة علمية منشورة وهي:

-ماريلين أورديكيان، "العملات الافتراضية المشفّرة في الحقل الجنائي السيبراني"، مجلة الدفاع الوطني، العدد 108، نيسان 2019، الصفحات 73-105، https://www.lebarmy.gov.lb/ar/content/108-d

[25] قانون رقم 81 تاريخ 10 تشرين الأول 2018، الجريدة الرسمية، عدد 45 تاريخ 18 تشرين الأول 2018، الصفحات 4546-4568 (قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي).

والعقوبات[26] وفي ظل عدم تغطية ومجاراة قوانينه الأفعال المقترفة بواسطة التقنيات الحديثة. وكنتيجة، تطرح الأسئلة نفسها، ما هي العملات التشفيرية؟ هل هي مال؟ ما طبيعتها؟ كيف تختلف عن النقود الرسمية؟ هل هي آمنة؟ ما مخاطرها؟ ما مدى شرعيتها؟ هل من الضروري تنظيمها قانوناً؟ ما هي الآليات المعتمدة على تنظيمها؟ وفي أي إطار قانوني يتم التطرق إليها؟ هل يتم استعمالها في المسائل غير المشروعة؟ ما هي العوامل التي تجعلها مرغوبة من قبل المجرمين؟ ما دورها في عالم الجريمة؟ كيف يؤثر تنظيمها قانوناً على الظاهرة الجرمية بحد ذاتها؟ كل هذه الإشكاليات تمهّد إلى الإشكالية الرئيسية وهي، هل العملات التشفيرية هي عملة المستقبل أو عملة المجرمين؟

كل هذه التساؤلات سنحاول الإجابة عنها في معرض الدراسة، عبر عرض المواد القانونية ومن ثم تحليلها وتفسيرها، بحيث يُخصص القسم الأول لدراسة الإطار القانوني للعملات التشفيرية بينما يُخصص القسم الثاني لدراسة جرائم العملات التشفيرية، عسى أن نتوصل إلى إجابات واضحة واستنتاجات ومقترحات في الخاتمة.

[26] تنص المادة الثامنة من الدستور اللبناني تاريخ 23 أيار 1926، على ما يلي:
"الحرية الشخصية مصونة وفي حمى القانون ولا يمكن أن يقبض على أحد أو يحبس أو يوقف إلا وفاقاً لأحكام القانون ولا يمكن تحديد جرم أو تعيين عقوبة إلا بمقتضى القانون."

القسم الأول: الإطار القانوني للعملات التشفيرية

إبّان الأزمة الاقتصادية العالمية والانهيارات المالية والمصرفية، تلقى بتاريخ 31 تشرين الأول من العام 2008 مئات المهتمين وخبراء التشفير بريداً إلكترونياً من شخص (أو جهة) مجهول يطلق على نفسه اسم ساتوشي ناكاموتو **Satoshi Nakamoto**، يتحدث عما سمّاه في ورقته البيضاء بـ "البيتكوين: نظام النقد الإلكتروني من نظير إلى نظير"[27]. يقول "ناكاموتو" في البريد الإلكتروني بأنه "كان يعمل على نظام نقد إلكتروني جديد قائم كلياً على النظير للنظير يستبعد جهة ثالثة موثوق بها"[28]. تشرح ورقته البيضاء المؤلفة من تسع صفحات نظامه الرقمي لعملة، معتمداً على المعادلات والرموز والمراجع، وصرّح بأنه "يفسّر العملة الإلكترونية بأنها سلسلة من التواقيع الرقمية... بحيث يُرسل مالك العملة عملته إلى شخص آخر عبر توقيعه إلكترونياً الهاش **Hash** التابع لعملية التحويل السابقة والمفتاح العام للمالك اللاحق، ويضاف ذلك إلى نهاية العملة. يمكن للمستفيد أن يصدّق على التوقيع ليصدّق تبعاً على سلسلة الملكية"[29]. في صميم عملة "ناكاموتو" يقوم سجل عام علني بالكامل وغير قابل للتعديل، يعتبر هذا السجل الذي أُطلق عليه لاحقاً تسمية البلوكشاين (سلسلة الكتل) **Blockchain**، عبارة عن عرض رقمي وموضوعي للحقيقة الكاملة في النظام.

باختصار، عرض "ناكاموتو" نظام تبادل على شبكة الإنترنت مبني على التشفير، يسمح لجهتين من تبادل قيمة معينة من دون الإفشاء عن بياناتهم الشخصية أو المرتبطة بحساباتهم المالية.

في البداية، لم يتجاوب أحد مع "ناكاموتو" معتبرين بأن ما يعرضه ليس إلا تكرار للمحاولات السابقة التي بائت بالفشل، لحين بداية العام 2009 بحيث أقدم "ناكاموتو" على تعدين عملة البيتكوين وكوّن أول

[27] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, p. 1, www.bitcoin.org.

[28] https://satoshi.nakamotoinstitute.org/emails/cryptography/1/

[29] Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System,” p. 2.

كتلة المعروفة بكتلة التكوين **Genesis Block**، ولكن كان نظام "ناكاموتو" على وشك الفشل من دون جهة ثانية على الشبكة تُقدم على تجربة نظامه وشبكته ويتم تبادل العملات فيما بينهم. هنا يأتي المبرمج هال فيني **Hal Finney**، الذي بادر وتواصل مع "ناكاموتو" وحمّل برنامج البيتكوين على حاسوبه فبدئا بتجربة هذا النظام، وبعد تجارب عديدة أصبح فيني أول مُستقبل للبيتكوين في العالم.

سرعان ما تفشّت ظاهرة البيتكوين وبدأت جهات أخرى من استغلال برنامجها ذات المصدر المفتوح **Open Source** ومن إصدار عملات تشفيرية مماثلة، أولها كانت عملة نايمكوين **Namecoin** لحقتها مئات العملات التشفيرية التي تتمتع بخصائص مماثلة ومختلفة للبيتكوين.

من هذا المنطلق، كان من الضروري البحث بالتالي:

الباب الأول: مفهوم العملات التشفيرية

الباب الثاني: تَبعة المفاعيل التطبيقية للعملات التشفيرية

الباب الأول: مفهوم العملات التشفيرية

يكشف تاريخ المال عن تحدٍ رئيسي وهو كيفية تصميم نظام يسهّل بطريقة أكثر فاعلية تبادل السلع والخدمات ويولد الازدهار الاقتصادي، مع منع المؤسسات التي تدير هذا النظام من إساءة استخدام الثقة الممنوحة لهم جراء دورهم هذا، فالثقة بالمؤسسات المالية وبالدولة وبعملتها هي أساس الثقة بالنظام النقدي من أساسه. ولقد برهن التاريخ بأن هذه الثقة يمكن فقدانها وكسبها بوهلة، ففقدانها يعني الدمار الاقتصادي وانهيار النظام النقدي، وكسبها يعني الاستقرار والازدهار والتمتع بالسلطة بحد ذاتها.

أما إذا كانت عملة البيتكوين أو سائر العملات التشفيرية تمثل حلاً قابلاً للتطبيق لهذا التحدي، فذلك موضوع يستوجب البحث في الوقت الراهن. تكمن الخطوة الأولى للعملات التشفيرية نحو هزم هذا التحدي هو أن يتم قبولها على نطاق واسع كأموال قادرة على البقاء، أي تصبح وسيلة موثوق بها لتوسيع التبادل والازدهار[30].

لا شك بأن أول عملة تشفيرية أي البيتكوين، وضعت نظاماً حديثاً على صعيد العملات الرقمية والإلكترونية والنظام النقدي المالي، فهذا النظام نقض المحاولات السابقة لإنشاء عملات رقمية، فهو سلب عنصر الثقة من المؤسسة المالية والدولة ومنحها إلى الجميع عبر كسره لقيود النظام المركزي المالي. فكيف لا يكون هذا النظام الحديث والفريد من نوعه بالنظام الثائر الذي يقلب مقاييس المال والأنظمة المالية والنقدية؟

البيتكوين ليست بعملة فقط، بل نظام مميز بحد ذاته وتقنية مبتكرة ارتكزت عليها العملات التشفيرية اللاحقة لها[31]، فلها سمات وخصائص عديدة مبنية على تقنيات ووسائل عصرية. لذلك ارتأينا بحث ماهية العملات التشفيرية في الفصل الأول لننتقل في الفصل الثاني للبحث حول الوصف القانوني للوسائل التقنية.

---

[30] Paul Vigna, and Michael J. Casey. **The Age of Cryptocurrency: How Bitcoin and The Blockchain are Challenging The Global Economic Order**, Picador, 2016, p. 39.

[31] البيتكوين ليست فقط بعملة رقمية تشفيرية ونظام دفع إلكتروني، بل تقنية جديدة قائمة بحد ذاتها في عالم التكنولوجيا.

الفصل الأول: ماهية العملات التشفيرية

عندما يأتي الأمر بالمصطلحات والتسميات، تهيمن الفوضى جرّاء التباين الكبير بالمصطلحات المستخدمة للدلالة إلى كل فئة من العملات الرقمية والتشفيرية. لتاريخنا لا توحيد قانوني أو تقني، والتباين يتعقّد أكثر ابّان إصدار قانون أو ورقة بحثية تُطلق مصطلحات جديدة.

في حين تتعدد وتختلف المصطلحات، هنالك فئات لا تكترث بالتسميات بل تهتم فقط بخصائص الابتكار القائم عليها نظام العملات التشفيرية، هذه الخصائص الفريدة من نوعها والتي جذبت الجميع تتراوح من تقنية بحت إلى اقتصادية ومالية.

وبالتالي، سنعالج في المبحث الأول المصطلحات والتعاريف المنسوبة إلى العملات التشفيرية مع التفريق بينها وبين سائر العملات والنقود الرقمية والافتراضية، لننتقل في المبحث الثاني إلى خصائص العملات التشفيرية والنظام الحديث القائمة عليه.

المبحث الأول: المصطلحات والتعريفات من الوجهة القانونية والفقهية

العملات الرقمية هي الأموال والأصول المستخدمة على شبكة الإنترنت. عرّفت مجموعة العمل المالي **FATF**[32] العملات الرقمية **Digital Currencies** على أنها في آن، تمثيل رقمي لعملة افتراضية (غير رسمية) والنقود الإلكترونية **E-money** (النقود الرسمية)[33]. على هذا المنوال، جعلت مجموعة العمل المالي من عبارة العملات الرقمية مصطلحاً عاماً يشمل في الوقت عينه أولاً النقود الرقمية الرسمية وثانياً تلك غير الرسمية الافتراضية. فيقتضي تفسير هذه العبارات وفقاً لآلية مجموعة العمل المالي لأنها

[32] Financial Action Task Force

[33] FATF. Report on **Virtual Currencies Key Definitions and Potential AML/CFT Risks**, France, June 2014, p. 4, http://www.fatf-gafi.org/publications

الأكثر تفصيلاً[34]، مستعينين ببعض مفاهيم المصرف المركزي الأوروبي **ECB** [35]، لنتطرق لاحقاً إلى مصطلحات وتعاريف تبنتها جهات أخرى.

أولاً. النقود الإلكترونية E-money:

النقود الإلكترونية أي **Electronic Money** (مختصر **E-money**) هي التمثيل الرقمي للنقود الورقية الرسمية، تُستخدم لنقل وتحويل قيمة معينة من النقود الرسمية إلكترونياً. هناك العديد من القوانين المحلية والإقليمية التي ترعى وتنظّم النقود الإلكترونية، منها التوجيه الأوروبي للنقود الإلكترونية رقم EC/110/2009 تاريخ 16 أيلول 2009 [36]. عرّفت المادة الثانية من التوجيه الأوروبي المذكور، النقود الإلكترونية على أنها:

"'electronic money' means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer;"

---

[34] سنعتمد على آلية الشرح المذكورة في تقرير مجموعة العمل المالي لعام 2014، فهذا التقرير يعتبر الأساس الذي استندت عليه المجموعة لإصدار التوصيات والإرشادات والتعديلات اللاحقة.

[35] European Central Bank

[36] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, **Official Journal of the European Union**, L.267/7, 10 Oct. 2009.

يقتضي التنويه على أن العملات التشفيرية وسائر أنواع العملات والأصول الافتراضية ليست بنقود إلكترونية، فهذه الأخيرة تُعد نقوداً رسمية وهي بحمى كافة القوانين والأنظمة المالية المحلية والعالمية. وبالتالي، إن هذه النقود هي مستبعدة من نطاق الدراسة.

ثانياً. العملات الافتراضية Virtual Currencies أو الأصول الافتراضية Virtual Assets:

تغيّرت التعاريف والمصطلحات المعتمدة من قبل مجموعة العمل المالي على مدار السنين، فبعد أن استهلّت بمصطلح "العملات الافتراضية" في أول تقرير لها في هذا الشأن في العام 2014، عادت وعدّلت المصطلح في شهر تشرين الأول من العام 2018 واستبدلته بـ "الأصول الافتراضية" **Virtual Assets** [37]، وعرفتها على أنها:

"A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."

وعليه، تنقسم العملات الرقمية الافتراضية إلى نوعان[38]: (أ) غير قابلة للتحويل **Non-Convertible** (ب) قابلة للتحويل **Convertible**، وسنقوم بمناقشتها تبعاً:

أ) **العملات غير القابلة للتحويل Non-Convertible:** هي تلك التي لا يمكن تبديلها مع النقود الرسمية، فنطاقها مقتصر في عالم افتراضي معيّن. فرّق المصرف المركزي الأوروبي **ECB** بين نوعين من العملات

---

[37] FATF. "Regulation of Virtual Assets," France, 19 Oct. 2018, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/regulation-virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

[38] FATF. Report on **Virtual Currencies**, 2014, Op.cit., p. 4.

الافتراضية غير القابلة للتحويل[39] وهي إما (1) مغلقة **Closed** وإما (2) ذات التدفق الأحادي **Unilateral Flow**.

1) **المغلقة Closed**: هذا النوع موجود في الإجمال في الألعاب الإلكترونية والافتراضية مثل **World of Warcraft Gold**. إن هذه الالعاب مجانية، الا أنه وفي بعض الأحيان يكون هناك رسم انضمام إلى شبكة اللعبة. يكتسب اللاعب كمية محددة من العملة عند تحقيق إنجازات معينة والوصول إلى مستوى متقدم من اللعبة، فتأتي العملة على سبيل المكافأة.

2) ذات التدفق الأحادي Unilateral Flow: يتم الاستحصال على هذا النوع من العملات عبر شرائها بالنقود الرسمية[40]، أي يمكن تحويل النقود الرسمية إلى هذا النوع ولهذا السبب سُميت بالعملات ذات التدفق الأحادي. تمكّن هذه العملات من شراء السلع والبضائع والخدمات الموجودة داخل النطاق المحدد للعملة، غالباً من متجر إلكتروني الخاص. من هذه العملات نذكر **Riot Points RP** في لعبة **League of Legends** الشهيرة والـ **Reddit Coins** المستعملة على شبكة التواصل **Reddit**. فعلى سبيل المثال، يمكن الاستحصال على 500 **Reddit coins** من المتجر الخاص بالشبكة مقابل 1.99 دولار أميركي[41].

بيد أن بعضاً من هذه العملات المركزية أصبحت قابلة للتحويل خلافاً لطبيعتها ونظامها، وذلك جراء ظهور سوق سوداء تُجيز باستبدالها بنقود رسمية أو الإقدام على مقايضتها بسلع أخرى.

ب) **العملات القابلة للتحويل Convertible:** هي عملات يمكن الاستحصال عليها بالنقود الرسمية ويمكن إعادة تبديلها بهذه الأخيرة، وذلك لقاء سعر صرف معيّن[42]، فهي تتمتع بقيمة معادلة لهذه النقود وتمكّن

---

[39] ECB. **Virtual Currency Schemes**, October 2012, pp. 13-15, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[40] ibid., p. 14.

[41] https://www.reddit.com/coins

[42] عرّف المصرف المركزي الأوروبي هذه العملات بالعملات ذات التدفق الثنائي الازدواجي "Bidirectional Flow".
-ECB. **Virtual Currency Schemes**, 2012, Op.cit., p. 14.

من شراء السلع والخدمات سواء في العالم الافتراضي أو العالم المادي الحقيقي. ولكن إن قابلية التحويل هذه ليست مرعية بالقوانين، واستمرارية هذه الميزة معلّقة بوجود سوق متاح يقبل بهذا التحويل.

إن العملات القابلة للتحويل هي على نوعين[43]، الأولى مركزية **Centralised** والثانية غير مركزية **Decentralised** (وهي موضوع رسالتنا الراهنة):

1) تنشأ وتُدار العملات المركزية القابلة للتحويل مثلها مثل العملات المركزية غير القابلة للتحويل، من قبل سلطة مركزية معينة ومحددة. تُقدم هذه الإدارة المركزية التي تُعتبر جهة ثالثة، على تحديد النظام الخاص بالعملة وأسس تداولها واستعمالها وتسهر على مواكبتها وتطويرها. يكون سعر صرف هذه العملات إما ثابتاً **Fixed**، أي يُحدد من خلال معادلته مع قيمة عملة رسمية معينة أو أي شيء آخر ذو قيمة مثل الذهب والفضة إلخ. أو يكون عائماً **Floating**، يُحدد بموجب آلية العرض والطلب في السوق. من هذه العملات نذكر الـ **E-Gold** التي كانت مدعومة بالذهب الحقيقي[44].

2) العملات غير المركزية أي العملات التشفيرية، عبارة عن عملات موزّعة ذات المصدر المفتوح، قائمة على نظام النظير للنظير أو الند للند بموجب معادلة رياضيات. ليست هناك من سلطة مركزية تديرها أو تراقبها أو تشرف عليها[45].

- <u>**موقف المصرف المركزي الأوروبي ECB:**</u> في أوّل تقرير له في العام 2012، اعتُمد مصطلح العملات الافتراضية "**Virtual Currencies**" تماماً مثل مجموعة العمل المالي، ولقد قُسّمت العملات الافتراضية إلى ثلاث فئات (تمت معالجتها في الفقرة السابقة) وهي العملات ذات التدفق الثنائي الازدواجي **Bidirectional Flow**، العملات المغلقة **Closed** والعملات ذات التدفق الأحادي **Unilateral Flow**. عرّف التقرير الأول مصطلح العملات الافتراضية على أنها نوع من النقود الإلكترونية غير المنظمة

---

[43] FATF. Report on **Virtual Currencies**, 2014, Op.cit., p. 5.

[44] تم تأسيسها في العام 1996 من قبل Gold & Silver Reserve Inc. التي كانت تديرها لحين إغلاقها جراء مشاكل قانونية وقضائية.

[45] FATF. Report on **Virtual Currencies**, 2014, Op.cit., p. 5.

قانوناً، تصدر وغالباً ما تُدار من قبل مطوريها ومبرمجيها **Developers**، ويتم استعمالها والقبول بها وسط أفراد تابعين إلى مجتمع افتراضي معيّن[46].

إلا أنه وبعد عدة تقارير ودراسات، اعتمد المصرف المركزي الأوروبي مصطلح "الأصول التشفيرية" **Crypto-Assets** بدلاً من "العملات الافتراضية غير المركزية"، بحيث حصر المصطلح ودراساته بالعملات التشفيرية دون سائر العملات الرقمية الافتراضية. لقد عرّفت وحدة الأصول التشفيرية التابعة للمصرف المركزي الأوروبي **Crypto-Assets Task Force** في تقريرها لعام 2019، على أنها[47]:

"A new type of asset recorded in digital form and enabled by the use of cryptography that is not and does not represent a financial claim on, or a liability of, any identifiable entity."

- **التوجيه الأوروبي الخامس لمكافحة تبييض الأموال AMLD 5** [48]**:** اعتمد الاتحاد الأوروبي مصطلح العملات الافتراضية **Virtual Currencies** حين وسّع في العام 2018 بموجب التوجيه الخامس لمكافحة تبييض الأموال **AMLD 5** [49]، نطاق التوجيه الرابع ليشمل العملات الافتراضية. يضع هذا التوجيه مع

---

[46] "A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".

-ECB. **Virtual Currency Schemes**, 2012, Op.cit., p. 13.

[47] European Central Bank Crypto-Assets Task Force. Paper on **Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures**, No. 223, May 2019, p. 3, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

[48] Fifth Anti-Money Laundering Directive

[49] Council of Europe: Directive 843\2018 of the European Parliament and of the Council of 30 May 2018 amending Directive 849\2018 on the prevention of the use of financial system for the purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, **Official Journal of the European Union**, L.156, 19 Jun. 2018.

تعديلاته السابقة واللاحقة، الأساس القانوني المعتمد في أوروبا لمنع استغلال النظام المالي في أنشطة تبييض الأموال وتمويل الإرهاب. تكمن أهمية هذا التوجيه بإدخاله لأول مرة مصطلح العملات الافتراضية ليصبح التوجيه منطبقاً عليها. ولقد عرّفها بموجب المادة الأولى فقرة (2) (d)(18) على أنها تمثيل رقمي لقيمة غير صادرة أو مدعومة من مصرف مركزي أو سلطة عامة، ولا ترتبط بعملة منشأة قانونًا ولا تتمتع بالوضع القانوني لعملة أو النقود، ولكن يتم قبولها كوسيلةٍ للتبادل من قبل أشخاص طبيعيين أو معنويين ويمكن نقلها وتخزينها وتداولها إلكترونياً[50].

– **<u>شبكة FinCEN الأميركية:</u>** في العام 2019، أصدرت شبكة **FinCEN** الأميركية[51] إرشادات تفسيرية تحت عنوان "**Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies**"[52]، تتناول مدى تطبيق قانون السرية المصرفية ولوائحه التنفيذية على نماذج أعمال معينة تنطوي على عملات افتراضية قابلة للتحويل. اعتمدت شبكة **FinCEN** مصطلح العملات الافتراضية القابلة للتحويل **CVC**[53]، وعرفتها على أنها نوع من العملات

---

[50] art. 1 (2)(d)(18) of AMLD 5:

""virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."

[51] Financial Crimes Enforcement Network

[52] FinCen. "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", FIN-2019-G001, 9 May 2019, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models

[53] Convertible Virtual Currencies

الافتراضية إما أن لها قيمة معادلة كعملة، أو تعمل كبديل للعملة، وهي بالتالي نوع من "قيمة تحل مكان عملة"[54].

- **هيئة الأوراق المالية والبورصات الأمريكية SEC:** أصدرت هيئة الأوراق المالية والبورصات الأمريكية **SEC** [55] في العام 2019، إرشادات تحت عنوان "**Framework for Investment Contract Analysis of Digital Assets**"[56]. لقد تبنّت مصطلح "أصول رقمية" **Digital Assets** للدلالة على العملات التشفيرية، بحيث عرفتها على أنها أصول يتم إصدارها ونقلها باستخدام تقنية السجل الموزّع أو البلوكشاين، بما في ذلك، على سبيل المثال لا الحصر، ما يسمى "العملات الافتراضية" و"العملات المعدنية" و"الرموز"[57].

- **قانون PACTE الفرنسي[58]:** عدّل قانون **PACTE** الفرنسي نصوص عديدة من قانون النقد والمال الفرنسي، ولقد تحدّثت المادة 86 منه عن مقدمي خدمات الأصول الرقمية "**Prestataires de Services Sur Actifs Numériques**" وعرّفت مصطلح الأصول الرقمية "**Actifs Numériques**" على أنها تمثيل رقمي لقيمة غير صادرة أو مدعومة من قبل مصرف مركزي أو سلطة

54 "CVC is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency"."
-FinCEN. Op.cit., p. 7.

55 U.S. Securities and Exchange Commission

56 U.S. SEC. "Framework for "Investment Contract" Analysis of Digital Assets," 3 Apr. 2019, https://www.sec.gov/files/dlt-framework.pdf

57 "The term "digital asset," as used in this framework, refers to an asset that is issued and transferred using distributed ledger or blockchain technology, including, but not limited to, so-called "virtual currencies," "coins," and "tokens"."
-U.S. SEC, ibid., p. 12.

58 LOI no. 2019-486 du 22 Mai 2019 relative à la croissance et la transformation des entreprises (1), JORF No. 0119 du 23 Mai 2019, texte No. 2,
https://www.legifrance.gouv.fr/eli/loi/2019/5/22/ECOT1810669L/jo/texte

عامة، وليست بنقود رسمية ولا تتمتع بالصفة الرسمية، ولكن يتم القبول بها من قبل أشخاص طبيعيين أو معنويين كوسيلة للتبادل والتخزين والتحويل بشكل رقمي[59].

– **قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم 2018/81**[60]**:** عرّفت المادة الأولى من القانون المذكور مصطلح "النقود الالكترونية والرقمية" مع ترجمته بالفرنسية "**Monnaie et numérique Électronique** " وبالإنكليزية "**Digital or Electronic Money**" على أنها "وحدات تسمى وحدات نقد الكتروني يمكن حفظها على دعامة الكترونية". وسيتم البحث في هذا الموضوع بالتفصيل في الفصول القادمة.

– أما العملة التشفيرية **Cryptocurrency** كالبيتكوين، فهي بدورها نوع من أنواع العملات الرقمية[61]، ولكن تستخدم فيها تقنيات التشفير، لتنظيم توليد وحداتها والتحقّق من تحويل الأموال، وهي قائمة بشكلٍ مستقل عن أي مصرف مركزي. وعلى هذا الأساس، إنّ اعتماد هذه التقنية التي تُدعى تقنية البلوكشاين **Blockchain Technology** تجعل من العملات التشفيرية نظامًا نقدياً إلكترونياً مستقلاً، يعتمد في

---

[59] art. 86: “art. L. 54-10-1.- Pour l'application du présent chapitre, les actifs numériques comprennent:

…

2- Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.”

[60] قانون رقم 81 تاريخ 2018/10/10، الجريدة الرسمية، عدد 45 تاريخ 2018/10/18، الصفحات 4546-4568 (قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي).

[61] Robby Houben, and Alexander Snyers. Study requested by the European Parliament's TAX3 Committee, on “**Cryptocurrencies and Blockchain Legal Context and Implications for Financial-Crime, Money Laundering and Tax Evasion**,” No. PE 619.024, Brussels, July 2018, p. 20, http://www.europarl.europa.eu/committees/en/supporting-analyses-search.html

المعاملات المالية **Transactions** على مبدأ النظير للنظير **Peer to Peer** (مختصر **P2P**) وهو مصطلح تقني بحت مفاده التعامل المباشر بين مستخدم وآخر من دون الحاجة إلى وجود أي وسيط كالمصرف.

ومن المصطلحات والتعريفات العديدة والمتنوعة، ننتقل للبحث بأهم الخصائص التي تتصف بها العملات التشفيرية وذلك للدور البارز التي تلعبها هذه الخصائص في بلورة مفاعيلها.

المبحث الثاني: الخصائص التي تتفرّد بها العملات التشفيرية

تتصف العملات التشفيرية بخصائص تميّزها عن سائر العملات الرقمية الافتراضية والنقود الرسمية. فتنبثق هذه الخصائص من تقنيات حديثة ونظام مميّز لآلية العمل، يُعد بحد ذاته ابتكاراً تتخطى آثاره حدود الأجهزة الإلكترونية وشبكة الإنترنت، لا بل مزايا هذا النظام هي التي تستقطب وتشكّل الدافع لظاهرة الإقبال المكثّف.

سنتخذ في هذا المبحث عملة ونظام البيتكوين نموذجاً.

أولاً. أهم خصائص نظام البيتكوين:

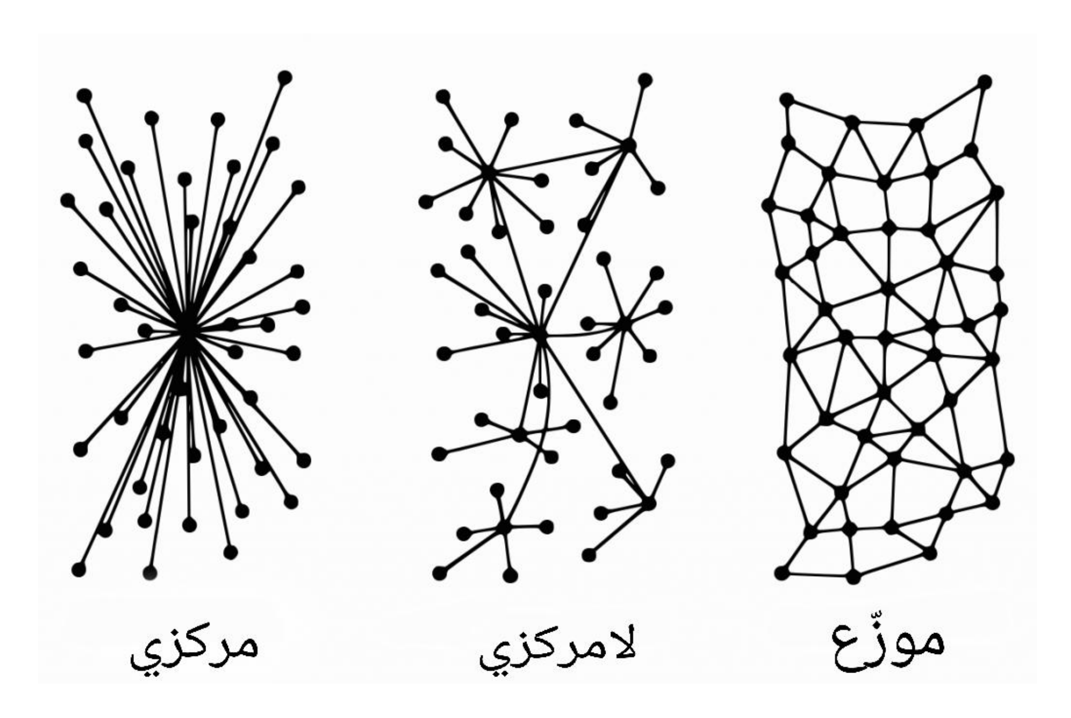
أ) اللامركزية Decentralisation:

نظام اللامركزية هي إحدى السمات الرئيسية والعبقرية التقنية التي خلفتها البيتكوين، والتي جعلت منها في آن عملة ونظام دفع. إن النظام المالي التقليدي المبني على عنصر "الثقة"، قائم على سجلات مركزية مملوكة وبحيازة المصارف والمؤسسات المالية. من إحدى علّات هذا النظام بأنه يمنح سلطة عظمى وأرباحاً خيالية لهذه الجهات المركزية التي تحتفظ بالسجلات[62]. في السنوات الأخيرة، تضخّمت قوة المصارف صاحبة هذه السجلات بحيث أصبح هناك تعويل واتّكال مباشر عليها عند الرغبة بإنجاز عملية

[62] Vigna, and Casey. **The age of cryptocurrency**, Op.cit., p. 121.

مالية معينة، فأضحى الاقتصاد العالمي وترابطه معتمداً تماماً على وساطة المصارف، وهذا ما أفضى إلى تدهور الاقتصاد العالمي في العام 2008 [63].

هنا أتى ساتوشي ناكاموتو واقترح في ورقة البيتكوين البيضاء استقصاء هذه السلطات المركزية واعتماد اللامركزية، بحيث قال "نحتاج إلى نظام دفع إلكتروني مبني على الدليل المشفّر بدلا من الثقة، بحيث يتمكن فريقان من اجراء التحويلات مباشرة فيما بينهما من دون الحاجة إلى جهة ثالثة موثوقة"[64]. وهكذا، استبعد نظام البيتكوين الأشخاص الثالثين الوسطاء، وأعطى سلطة إدارة السجلات إلى "عامة الشعب" [65]، فالسجل عام **Public** وغير سري وموزّع **Distributed**، لأنه قائم على شبكة النظير للنظير **P2P** منتفعاً من تقنية التشفير.



1. أنواع الشبكات[66]

[63] id., pp. 4,5.

[64] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, p. 1, www.bitcoin.org.

[65] Vigna, and Casey. **The age of cryptocurrency**, Op.cit., p. 5.

[66] Paul Baran. Report **On distributed communications: I. Introduction to distributed communications networks**, United States Air Force Project RAND, RM-3420-PR, 1964, p. 2.

ب) <u>التعدين Mining– نظام الإصدار والتصديق والتوثيق:</u>

في النظام المالي التقليدي، تصدر النقود الرسمية عن سلطة مركزية معينة مثل مصرف لبنان الذي يتمتع حصراً بصلاحية إصدار الليرة اللبنانية. أما البيتكوين، فهو نظام موزّع يعتمد على شبكة النظير للنظير فلا من مصرف أو سلطة مركزية يصدره، بل يكمن الإصدار بعملية التعدين **Mining** التي تعتبر الطريقة الوحيدة لإصدار عملة بيتكوين جديدة[67]. ينطوي التعدين على تنافس المعدنين أو "العقود" **Nodes** لإيجاد حلول لمسألة حسابية أثناء معالجة المعاملات **Transactions**. يجوز لأي شخص يستخدم جهازاً يشغّل كامل بروتوكول البيتكوين أن يكون معدناً، وذلك عبر استغلال قوة معالجة جهازه **CPU Power** [68] لتصديق المعاملات وتسجيلها على السجل العام[69]. فكلما حوّل شخص مبلغاً إلى شخص آخر، يمكن لجميع أعضاء الشبكة التحقق من أن المرسِل لديه رصيد كافٍ، وتبعاً تتنافس العُقد لتكون أول من يقوم بحل المسألة الحسابية بشكل صحيح وتحديث سجل البلوكشاين بكتلة جديدة من المعاملات. وهذا باختصار هو نظام "اثبات العمل" **Proof of Work**[70] **(PoW)**، بحيث يتم التصديق من قبل الجميع على هذه الكتلة الصحيحة التي يبثها المعدّن على الشبكة (ويُعرف هذا بمبدأ التراضي **Consensus**).

في نهاية هذه العملية التي تستغرق حوالي العشر دقائق، يُكافئ المعدّن ببيتكوين جديد[71]. يتضمن بروتوكول البيتكوين خوارزميات **Algorithms** [72] تنظم وظيفة التعدين عبر الشبكة[73]، وإن هذا البروتوكول

---

[67] Arvind Narayanan, et al. **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**, Princeton University Press, 2016, p. 73.

[68] Central Processing Unit

[69] Andreas M. Antonopoulos. **Mastering Bitcoin: Programming The Open Blockchain**, "O'Reilly Media, Inc.", 2nd edition, 2017, pp. 1,2.

[70] Saifedean Ammous. **The Bitcoin Standard: The Decentralized Alternative to Central Banking**, John Wiley & Sons, 2018, pp. 170,171.

[71] حالياً، يُكافئ المعدّن بـ 12.5 بيتكويناً.

[72] إن خوارزمية البيتكوين هي الـ SHA-256.

[73] Antonopoulos. **Mastering Bitcoin**, Op.cit., p. 2.

يقسّم الوتيرة التي "تنتج" بموجبها البيتكوين مع كل 210،000 كتلة مصدقة أي حوالي كل أربعة سنوات[74]، مما يعني وجود ضابطٍ للإصدار أي كمية محددة من البيتكوين التي يمكن تعدينها[75].

ج) __السجل العام Public Ledger:__

منذ القِدم، للسجلات والقيود الأهمية القصوى، لمَ؟ إن تبادل الخدمات والسلع حدد نطاق توسع المجتمعات وانفتاحها اقتصادياً، وكان ذلك ممكناً عبر تسجيل المواطنين (لاحقاً المصارف والمؤسسات المالية) ومتابعة ما لهم وما عليهم في هذه السجلات. يتمتع هذا السجل بثقة المجتمع... ثقة بمعنى أن محتواه هو الصحيح ويترجم الحقيقة. ولكن وفي نظامٍ مالي مركزي، هنالك سلطة مركزية هي التي تدير وتحتفظ بهذه السجلات؛ وهذا بالأمر الخطير لأن المجتمع وضع ثقته بهذه السلطة المركزية التي بإمكانها أن تتلاعب بهذه القيود متى شاءت، وهذا ما حصل بالتحديد في العام 2008 عندما خان العديد ومنهم المصرف الأميركي **Lehman Brothers** ثقة المجتمع وساهم بإحداث الأزمة الاقتصادية الخانقة. استغل المصرف المذكور الثقة المعطاة له من قبل المستثمرين والمساهمين والمشرع والجمهور، فلقد تبين تلاعباً جسيماً بسجلاته، خصوصاً عند إعلان إفلاسه بعد سنة "مربحة" وصلت فيها الأرباح إلى 4.2 مليار دولار[76].

استبعد ساتوشي ناكاموتو هذه المخاطر عبر استغلال تقنيات حديثة متمثلة بـ: شبكة النظير للنظير الموزّعة من دون نقطة فشل واحدة، التجزئة **Hashing**، التوقيع الإلكتروني ونظام إثبات العمل**PoW** [77].

على غرار ذلك، إن بروتوكول وبرنامج البيتكوين هو ذات المصدر المفتوح **Open Source**، فيمكن لأي

---

[74] Narayanan, et al. **Bitcoin and cryptocurrency technologies**, Op.cit., pp. 72,73.

[75] هنالك فقط 21 مليون بيتكوين، وبتاريخ إجراء هذه الدراسة، تم تعدين ما يقارب 17.9 مليون بيتكوين.

[76] Michael J. Casey, and Paul Vigna. **The Truth Machine: The Blockchain and the Future of Everything**, St. Martin's Press, New York, February 2018, pp. 18,24.

[77] Ammous. **The bitcoin standard**, Op.cit., pp. 170,171.

أحد أن يحمّله على حاسوبه، وبعد الاتصال بشبكة الإنترنت، يمكنه الانضمام إلى النظام اللامركزي العلني، ويصبح معدّناً يصدّق ويسجّل كافة العمليات.

ما يعزز الثقة بتقنية البلوكشاين بأنه يمكّن فقط إضافة المعلومات على السجل العام من دون امكانية ازالتها أو تعديلها. هذه الأمر في بالغ الأهمية، فلا مجال للعودة والتلاعب بالقيود المسجلة مسبقاً، فما تم تصديقه هو الحقيقة المجردة من دون أي فسحة للشك[78].

ثانياً. أسباب الإقبال على البيتكوين وشبكة البلوكشاين بشكل عام:

أ) **انخفاض تكلفة المعاملات وسرعة إنجازها:**

نتيجةً لإقصاء الوسيط على شبكة البلوكشاين فإن رسوم المعاملات وعمليات التحويل منخفضة جداً، وذلك مقارنةً مع رسوم تحويل النقود الرسمية عبر الشخص الثالث الوسيط. فبإطاحة الشخص الثالث المتوسط بين المرسِل والمرسَل إليه، ينعدم المبرر لتسديد رسوم باهظة يتقاضاها هذا الأخير عند إتمام العمليات. فعلى شبكة البيتكوين، يمكن معالجة عملية معينة وإجراء التحويلات حتى من دون رسوم؛ ولكن لتحفيز المعدّنين وكطريقة لتعويضهم عن عملهم، يُشجّع المستخدم على تسديد رسم رمزي وبشكل طوعي، مقابل تسريع تأكيد وتصديق عمليته أي منح عمليته الأولوية في التصديق. فإذا شاء، يسدد المرسِل هذا الرسم الذي يُحدد بحسب حجم العملية التي يرغب بإجرائها وبحسب نسبة الضغط على الشبكة.

على سبيل المثال، إن وحدة قياس حجم عملية معينة **Transaction Size** هي البايت **Byte**، وإن متوسط حجم عملية واحدة تقدّر بـ 225 **bytes**، في المقابل يمكن إجراء عملية تحويل "مسرّعة" مقابل تسديد 22 ساتوشي **satoshi** [79] مثلاً مقابل كل بايت في عملية، فسيكون الرسم المسدد 4950 ساتوشي أي ما يعادل 0.495 سنتاً أمريكياً[80].

---

[78] Casey, and Vigna. **The Truth Machine**, Op.cit., p. 65.

[79] ساتوشي satoshi، هي أصغر فئة من عملة البيتكوين وتعادل 0.00000001.

[80] يمكّن موقع /https://bitcoinfees.earn.com من مراجعة الرسوم ونسبة الضغط على الشبكة بوتيرة مباشرة.

أما بالنسبة إلى الوقت المتوجب لإتمام عملية معينة، فيتراوح فقط بين العشر دقائق في المبدأ وبضعة ساعات. وكنتيجة، يمكن إرسال كمية غير محددة من الأموال وفي غضون دقائق مقابل رسم زهيد، وذلك على عكس عمليات التحويل عبر المصارف التي تتطلب معالجتها بضعة أيام في الإجمال لقاء نسبة مرتفعة من قيمة الأموال موضوع العملية المصرفية.

ب) العالمية والإتاحة Accessibility:

تتخطى البيتكوين الحدود الدولية والجغرافية فهي عملة عالمية وعابرة للحدود، فلا جهة معينة تصدرها وتسيطر عليها، ومن يديرها هم مواطنين من كافة أنحاء العالم. بروتوكول البيتكوين ذات المصدر المفتوح، فيمكن الوصول إلى البيتكوين وسائر العملات التشفيرية بسهولة بمجرد تحميل البرنامج الخاص على أجهزة حوسبة بما فيها الحواسيب والهواتف الذكية[81] وعبر الاتصال بشبكة الإنترنت، في أي وقت كان، بحيث يمكن تحويل البيتكوين بنقرة واحدة من أي مكان في العالم ومن دون الحاجة إلى التردد للمصرف أو فتح حساب لديه. يمكن الاستفادة من هذه الميزة في البلدان النامية بحيث يصعب الوصول إلى الخدمات المصرفية، أو البلدان التي تعاني من عدم استقرار نقدي.

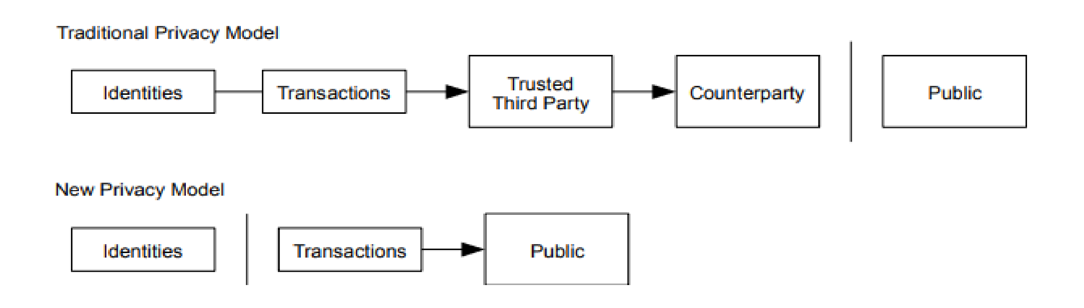
ج) الحفاظ على الخصوصية وإخفاء الهوية:

يصون نظام البيتكوين الخصوصية المالية والخصوصية الفردية عبر إضمار الهوية. ففي النظام المصرفي التقليدي، يكون الحساب دائماً مرتبطاً بهوية صاحبه، فتحقق الخصوصية عبر الحد من امكانية وصول الطرف المعني والشخص الثالث الموثوق به للمعلومات. في المقابل، وبالرغم من أن كل التحويلات والعمليات على شبكة البيتكوين هي علنية؛ تقوم الخصوصية عبر الدلالة للأطراف عبر عناوين مفاتيحهم، فالهوية في بروتوكول البيتكوين تتولّد عبر عناوين مشفّرة. يفسّر "ناكاموتو" بأنه "يمكن للعامة أن ترى عملية إرسال شخص ما مبلغاً معيناً إلى آخر، ولكن من دون معلومات تربط هذا التحويل بأي شخص"، ويواصل

---

[81] Antonopoulos. **Mastering Bitcoin**, Op.cit., p. 1.

الشرح بالقول بأنه " كجدارٍ إضافي للحماية، يجب استخدام زوج جديد من المفاتيح عند كل عملية تحويل وذلك للحؤول دون الربط والتوصل للشخص. فهنالك إمكانية لا يمكن تجنبها تسمح بالربط من خلال تحويلات متعددة المدخلات (**Inputs**)، والتي تكشف أن مدخلاتها تابعة للشخص عينه. يكمن الخطر في حالة الكشف عن مالك المفتاح، فإذا تم الكشف هناك إمكانية لإفشاء تحويلات أخرى تعود للشخص نفسه"[82].



2. مصوّر توضيحي من ورقة البيتكوين البيضاء[83]

د) **الشفافية وحرية الدفع:**

إن نظام البيتكوين هو نظام شفاف بطبيعته، فكل معلومة متاحة للعلن. فميزة لاانعكاسية **Irreversibility** الحوالات والعمليات[84]، والطبيعة العلانية وتطلّب الإجماع عند تصديق كل عملية على الشبكة، توفر الشفافية المطلقة، وتبني حاجزاً أمام امكانية التلاعب بالقيود المسجلة على السجل العام. بالإضافة إلى ذلك، عبر إبعاد الوسيط أو الشخص الثالث **Middleman** والنفقات المرفقة معه، تبشّر العملات التشفيرية من تخفيف وطأة الفساد الكائن داخل هذه المؤسسات المالية[85]. ترافق هذه الشفافية عملية التحويل والتداول من بدايتها إلى نهايتها، مما يعزز الثقة لدى العامة ويدفعهم بالتعامل مع البيتكوين

---

[82] Nakamoto. “Bitcoin: A Peer–to–Peer Electronic Cash System,” p. 6.

[83] Loc.cit.

[84] أي نهائية المعاملات وعدم القدرة على إعادة الحال كما في السابق.

[85] Vigna, and Casey. **The age of cryptocurrency**, Op.cit., p. 6.

والعملات التشفيرية القائمة على تقنية البلوكشاين، وذلك في أي وقت كان ودون سقف معين على المبالغ المتداولة.

يوفر هذا النظام السهولة بالتداول الآمن، ومنفذاً من القيود والشروط التي تضعها المصارف عند الرغبة بإجراء أي عملية مصرفية، فبكبسة زرٍّ ومن المنزل ومن دون حساب مصرفي، يمكن أن يحوّل المستخدم أي مبلغ كان إلى أي مكان في العالم من دون أي تبرير عن وجهة أو سبب العملية المالية أو الاستحصال على موافقة سابقة.

و) نظام آمن سيبرانياً ومضاد للإنفاق المضاعف:

نظام البيتكوين هو نظام آمن يحارب الفجوات الأمنية التي تعاني منها الانظمة المالية المركزية. فنظراً لطبيعة شبكة البلوكشاين القائمة على تعدد النسخ المحفوظة والمسجلة في عقود **nodes** موزّعة، فإن بيانات السجل هي محمية من الهجمات السيبرانية المركزية وذي المناعة من الفقدان في حال اصابة خلل معين لإحدى الأجهزة[86].

بالإضافة إلى ذلك، إن إحدى الدوافع الجوهرية لابتكار نظام البيتكوين تكمن في ابتداعه حلاً لمشكلة الإنفاق المضاعف **Double-Spending**، التي كانت تشتكي منها العملات الرقمية السابقة. تقترح ورقة البيتكوين البيضاء حل هذه المشكلة عبر اعتماد خادم ذي طابع زمني موزّع **Timestamp Server** حسب شبكة النظير للنظير وذلك لإنشاء الإثبات الحاسوبي للترتيب الزمني للتحويلات[87]. سنعالج موضوع الإنفاق المضاعف بالتفصيل في القسم الثاني.

---

86 Michèle Finck. Study requested by the European Parliament's the Panel for the Future of Science and Technology (STOA), on "**Blockchain and The General Data Protection Regulation: Can Distributed Ledgers Be Squared With European Data Protection Law?**" No. PE 634.445, Brussels, July 2019, p. 3.

87 Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System," Op.cit., p. 1.

علاوةً على ذلك، فالعملات التشفيرية تتمتع بمميزات تنبع عن تكريس بعضٍ من التقنيات المتطورة، ولهذه المميزات توصيف وتوابع قانونية بارزة، لذلك سنعمد إلى تفصيلها في الفصل التالي.

الفصل الثاني: الوصف القانوني للوسائل التقنية

وفّرت التقنيات الحديثة وشبكة الإنترنت غطاء من المجهولية **Anonymity** على المستخدمين، فهذا الغطاء الذي يحمي ويحجب هويات هؤلاء من العلن وتتصف به العملات التشفيرية، أفسح لهم المجال للإقدام بأفعال على الشبكة لا يتجرؤون على ارتكابها في العالم المادي الواقعي[88].

ومن جهتها، تتمتع العملات التشفيرية بتقنية لا تتصف بها سائر أنواع العملات الرقمية والافتراضية، وهي إمكانية تبديلها مع النقود الرسمية، مما يُفيد الاحتكاك المباشر مع العالم الواقعي. فالبعض يرى بأن هذه الميزة بحد ذاتها هي التي أطغت الطابع الجدي على العملات التشفيرية وأزالت عنها دمغة "الافتراضية". وعليه، سنبحث في المبحث الأول ميزة المجهولية بإيجابياتها وسلبياتها ومدى إمكانية إزالتها، لننتقل في المبحث الثاني للبحث بميزة التحويل والتبادل فيما بين العملات التشفيرية والنقود الرسمية ومدى تأثيرها على العالم خارج الإطار الافتراضي.

المبحث الأول: المجهولية Anonymity الرقمية والاسم المستعار Pseudonym

تصون ميزة المجهولية بشكل عام الخصوصية الرقمية[89] وتتصف بإيجابيات عديدة[90]، فهي تسمح للمستخدم بتصفّح شبكة الإنترنت من دون الإفصاح عن هويته ويبقى بمنأى من الرقابة والتعقّب الرقمي، أي تحمي حرمته الشخصية الإلكترونية الأمر الذي أضحى بشبه المستحيل في عصرنا الراهن. إلا أن هذه

---

[88] Eoghan Casey. **Digital Evidence and Computer Crime: Forensic Science, Computers, And The Internet**, Academic press, 2011, p. 671.

[89] Michel E. Kabay. "Anonymity and pseudonymity in cyberspace: deindividuation, incivility and lawlessness versus freedom and privacy." Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR), Vol. 16, 1998, p. 14. http://www.mekabay.com/overviews/anonpseudo.pdf

[90] مثلاً، يمكن للمستخدم الذي ينتمي إلى دولة تحّرم وتقيّد الحريات، أن يعبّر عن آرائه بكل حرية وامان ومن دون أن يتعرّض للملاحقة.

المجهولية استُغِلّت أيضاً في النشاطات غير المشروعة طبعاً لأنها تقلّص نسبة كشف هوية المستخدم من قبل السلطات المعنية، فتحوّلت إلى إحدى العوامل أو الوسائل المؤثرة في زيادة نسبة الجرائم السيبرانية، ولقد اعتبر البعض[91] بأن هذه الميزة قد تؤدي إلى انحراف في الأسلوب والنشاط على شبكة الإنترنت في حال اجتمعت مع عوامل حافزة أخرى. ونظراً لاتصاف العملات التشفيرية بميزة المجهولية، تبنّت فئة من المجرمين هذه العملات لإضفاء غطاء إضافي من المجهولية إلى أنشطتهم غير المشروعة[92].

إن طبيعة تقنية البلوكشاين القائمة عليها العملات التشفيرية تساهم بإضفاء هذه المجهولية، فعملية التعامل مباشرة من دون وسيط يؤدي إلى استبعاد طرق التعقّب والمراقبة المعتمدة في الأنظمة المالية التقليدية من قبل المصارف وسلطات إنفاذ القانون.

بالإضافة إلى ذلك، مقارنةً مع المعاملات المالية المصرفية، والتي تتطلب إبراز وثائق رسمية وبيانات شخصية لإثبات هوية المستخدم امتثالاً للأنظمة المصرفية، فإن نظام المعاملات الافتراضية لا يشترط إبراز هكذا وثائق أو تقديم بيانات تصرّح وتربط هوية المستخدم الحقيقي بحسابه المالي الرقمي[93].

وللبحث أكثر عن ميزة المجهولية عند العملات التشفيرية، سنتّخذ من عملة البيتكوين مثالاً تطبيقياً.

يُسجِّل البلوكشاين التابع للبيتكوين جميع المعاملات التي أجريت عبره أي يحفظ الآثار الرقمية لكافة الإجراءات والمعاملات، نظراً لكونه سجل عام مفتوح وعلني أمام العموم[94]. ولكن، السؤال الذي يطرح نفسه

---

[91] Jesse D. Bray. **Anonymity, Cybercrime, and the Connection to Cryptocurrency**, master's thesis, Eastern Kentucky University, 2016, p. 14, https://encompass.eku.edu/etd/344

[92] Perri Reynolds, and Angela SM Irwin. "Tracking Digital Footprints: Anonymity within The Bitcoin System." Journal of Money Laundering Control, Vol. 20.2, 2017. pp. 172-189, p. 172.

[93] باستثناء بعض منصات التداول التي تستوجب إبراز وثائق رسمية تثبت هوية المستخدم، وذلك امتثالاً منها لقواعد وانظمة مكافحة تبييض الأموال وتمويل الإرهاب. تجدر الإشارة إلى أنه قبل صدور التوجيه الأوروبي الخامس لمكافحة تبييض الأموال وتشريعات أخرى خاصة بالعملات التشفيرية، لجأت بعض هذه المنصات إلى التشريع الذاتي، وذلك بمبادرة لكسب ثقة الجمهور وتبيان مدى شفافية عملها، من هذه المنصات نذكر منصة Coinbase الأميركية.

[94] هذه الميزة تتمتع بها شبكات البلوكشاين كافة ولا تقتصر على تلك البيتكوين.

هنا، إذا ما كانت سجلات البلوكشاين الموثّقة علانية، كيف يكتسب المستخدم ميزة السرية والمجهولية؟ في الحقيقة، إن عملة البيتكوين بحد ذاتها لا تتمتع بصفة المجهولية المطلقة وهذه واقعة خاطئة يقع فيها العديد. فعلياً، إن بُنية البيتكوين بحد ذاتها تسهّل إخفاء هوية المستخدم الذي ليس ملزماً على إبراز أي دليل أو بيانات شخصية في المقام الأول لإنشاء حسابه، بحيث يتم التعامل على شبكة البلوكشاين عن طريق مفتاح خاص **Private Key** ومفتاح عام **Public Key** [95] أو ما يسمى بعنوان البيتكوين الخاص بكل مستخدم، فهذين المفتاحين يحققان شبه مجهولية وغفلية البيتكوين (يُعرَّف المستخدم باسم مستعار وهو عنوان المفتاح العام الخاص به). وبالتالي، في وقت تتصف كافة العمليات على البوكشاين بالعلانية، إلا أن هوية الأطراف تغدو مجهولة إلى حد كبير.

وعليه، ما درجة المجهولية التي توفرها العملات التشفيرية وخصوصاً البيتكوين؟ وهل من الممكن ازالتها أو التخفيف من درجتها؟ كما قلنا، إن عملة البيتكوين هي عملة "شبه مجهولة أو مغفلة"[96] وذلك جراء تغطية المستخدم هويته الحقيقية **باسم مستعار Pseudonym** المتمثّل بعنوانه الخاص أو مفتاحه

---

[95] ان نظام اعتماد مفتاحين، مفتاح خاص ومفتاح عام يُسمى بالتشفير اللامتماثل Asymmetric Cryptography. في هذا النظام، يكون المفتاح الخاص معروفاً من شخص أو جهة واحدة فقط، وهو المرسِل ويستخدم هذا المفتاح لتشفير الرسالة وفك تشفيرها.

أما المفتاح العام فهو معروف من قبل العموم، ويستطيع فك شيفرة الرسالة المشفّرة عبر المفتاح الخاص، ولكن ليس بمقدور أي جهة ما عدا الجهة التي شفرت الرسالة بالمفتاح الخاص أن تفك شيفرة الرسالة المشفرة بالمفتاح العام.

-يراجع:

د. حسين الغول، **جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها**، الطبعة الأولى، مكتبة بدران الحقوقية، 2017، ص. 93.

-أيضاً:

د. وسيم الحجار، **الاثبات الإلكتروني**، المنشورات الحقوقية صادر، 2007، ص. 191.

[96] FATF. Report on **Virtual Currencies**, 2014, Op.cit., p. 6.

-أيضاً:

-Joshua Brustein. “Bitcoin May Not Be So Anonymous, After All.” Bloomberg, 27 Aug. 2013, www.bloomberg.com/news/articles/2013-08-27/bitcoin-may-not-be-so-anonymous-after-all, Accessed 22 Oct. 2018.

العام[97]، والذي يعتبر بمثابة هوية المستخدم أو بطاقته التعريفية على البلوكشاين. ولقد اعتبر البعض[98] بأن حتى هذا القدر من المجهولية عند البيتكوين، يعتبر من العوامل الجاذبة والمحفّزة للمجرمين.

إذاً في هذه الحالة، كيف نربط عملية معينة بعنوان المستخدم الخاص وصولاً إلى كشف هويته الحقيقية؟ هنالك برامج تقنية تسمح بتعقّب المستخدم عن طريق السجل العام للبلوكشاين وذلك من خلال التحليل الدقيق للعمليات، بحيث تربط مفتاح المستخدم العام بهويته الحقيقية. نشير إلى أن إمكانية وفرص تعقّب المستخدم توصلاً إلى إزالة مجهوليته ترتفع، إذا ما كان هذا الأخير يجري سائر عملياته على الشبكة بواسطة ذات العنوان أو المفتاح العام[99]. ولهذا السبب، يعمد الكثر إلى تغيير عنوانهم قبل كل عملية، تفادياً لإمكانية الربط بين عملياتهم وهوياتهم.

نشير إلى أن إجراءات الكشف عن هوية المستخدم تكون أكثر سهولة، إذا ما كان هذا الأخير قد تعامل مع منصة تبادل إلكترونية **Exchange** أو مع مقدم خدمة المحفظة عبر شبكة الأنترنت **Online Wallet Service** أو بأصحاب المحلات والشركات ومواقع التجارة الإلكترونية الذين يطلبون الإفساح والابراز عن بيانات حقيقية ووثائق رسمية. ففي التجارة الإلكترونية على سبيل المثال، يكون المستهلك ملزماً على منح التاجر معلومات تتعلق بحسابه وبطاقته المصرفية لتسديد الثمن، وبيانات أخرى كعنوان منزله ليتمكن التاجر من توصيل المنتج اليه. وهكذا، وفي المقام الأول، يكتشف التاجر هوية المستهلك، أو على الأقل يستحوذ على بيانات شخصية جوهرية تدل على هويته بطريقة غير مباشرة. ومن جهة ثانية، تتمكن

---

[97] وهي سلسلة أرقام وأحرف عشوائية تتولّد بالتشفير.

[98] Steven David Brown. "Cryptocurrency and Criminality: The Bitcoin Opportunity." The Police Journal, Vol. 89.4, 2016, pp. 327–339.

[99] هنالك برامج تتعقب معاملات المستخدمين عبر شبكة البلوكشاين، وتحلل الاستخدام المتكرر لمفتاح عام محدد وتربط المعاملات عبر مجموعة بيانات للعثور على المستخدم. عند القيام بذلك، تكوّن صورة عن المكان الذي يتسوق فيه مثلاً هذا المستخدم، والمقدار الذي ينفقه الخ. يمكن لهذه البرامج أيضاً أن تربط بمعاملات خارجية (في حال وُجدت)، حيث يتم جمع بيانات شخصية بواسطة أطراف الثالثة.

جهات ثالثة من استغلال هذه المعلومات للكشف عن هذه الهوية... فما أن ربط المستخدم حسابه بأي معلومة أو بيانات شخصية، ازدادت فرص ازالة غطاء الاسم المستعار المتمثل بالعنوان الخاص به.

إلا أن هناك تقنيات تزيد من درجة المجهولية الرقمية فتعقّد عملية الكشف عن هوية المستخدم، وأُطلق على هذه التقنيات والبرامج تسمية الـ **Anonymiser** أو **Anonymising Tool**. هذه التقنيات هي عبارة عن برامج وأدوات إلكترونية مصممة في الباب الأول لتضليل وتشويش وإخفاء الجهة التي تصدر عنها عملية تحويل عملة تشفيرية معينة، أي وظيفتها إسدال الستار على المصدر، مع العلم بأن هنالك عملات تشفيرية والمعروفة بعملات الخصوصية **Privacy Coins** [100] توفر غطاء كامل من المجهولية من دون هذه التقنيات أو البرامج.

وفي طبيعة الحال استهوت هذه التقنيات والبرامج المجرمين، بالرغم من أن مبتكريها لم يصمموها لهذه الدوافع اطلاقاً. نذكر من هذه التقنيات والخدمات المحفظة المظلمة **Dark Wallet** وخدمات المزج **Mixing Services/Tumbler** ومتصفح طور **Tor Browser**. أدناه سنعمد إلى شرح كل واحدة منها بإيجاز:

<u>أولاً. المحفظة المظلمة Dark Wallet:</u>

هي عبارة عن محفظة إلكترونية تمكّن من إضفاء المجهولية على البيانات عن طريق تشويش معاملات البيتكوين المجراة على شبكة الإنترنت. إن الجماعات الإرهابية كتنظيم الدولة الإسلامية قد سبق واعتبرت المحفظة المظلمة وسيلة مثالية لتسهيل تلقي التبرعات من دون الكشف عن هوية المتبرعين[101].

---

[100] عملات الخصوصية Privacy coins هي عملات تشفيرية تتصف بخصائص تقنية إضافية تحمي خصوصية وهوية المتعاملين معها، فهي تتميّز عن سائر العملات التشفيرية بطريقة تعاملها و"إخفائها" للمعلومات والبيانات الناتجة عن المعاملات.

من أبرز هذه العملات نذكر عملة مونيرو Monero (XMR)، زي كاش Zcash (ZEC) وڤيرج Verge (XVG).

[101] Erin K. O'Loughlin and Dennis Lormel. "Terror Finance And Technology", *Bank of America*, West Coast AML Forum 2015 May 6-8, 2015.

ثانياً. خدمات المزج Mixing Services– Tumbler:

عبارة عن برامج تقوم على خلط حزمة من العملات التشفيرية فيما بينها لإضاعة الأثر الرقمي لكل منها. فيتم تشويش هذه الآثار الرقمية والتسبب بفقدانها عن طريق تأخير طرح معاملة معينة على البلوكشاين بعد مزجها مع عملات أخرى، أي يتم تضليل وإضاعة الآثار الدالّة عن جميع المراحل التي قطعت بها العملة التشفيرية من مصدر وحيازة ومعاملات، وذلك عبر المزج والخلط فيما بين العملات[102].

ثالثاً. متصفح طور Tor Browser:

برنامج طور **Tor** وما يُعرف ببوابة الإنترنت المظلم، عبارة عن برنامج مجاني مفتوح المصدر، وُجد في المقام الأول للحفاظ على خصوصية المستخدم عند اتصاله بشبكة الإنترنت. يهدف برنامج طور إلى إخفاء البصمة الرقمية الخاصة بالمستخدم مما يتيح له تصفح شبكة الإنترنت والتحميل بشكل مجهول، وبالتالي التهرب من الرقابة الرقمية المفروضة على الشبكة. يعتمد برنامج طور على عدة طبقات من التشفير بحيث يخفي في المقام الأول عنوان بروتوكول الإنترنت الـ **IP Address** الخاص بالمستخدم.

وعليه، تشكّل العملات التشفيرية تحدٍّ لحملات مكافحة الجرائم السيبرانية، وبالإجمال إلى التقدم المحقق في هذا المجال. لا مندوحة بأن ميزة المجهولية وخصوصاً التقنيات والبرامج التي تزيد من درجتها، تساهم باستعادة المستخدم حياته الرقمية الخاصة وحرمته الافتراضية التي سُلبت منه، وصحيح أن مجهولية العملات التشفيرية أعادت حرية الفرد بالتصرف بأمواله على شبكة الإنترنت من دون رقابة أو قيود... ولكن في المقابل تساهم المجهولية بشكل عام بارتفاع نسبة الجرائم السيبرانية، وبشكل خاص باجتذاب المجرمين إلى العملات التشفيرية بل حتى أنها تعزز إرسال التبرعات إلى الجماعات الإرهابية[103] وعمليات تبييض الأموال. وبالرغم من إجراء الأبحاث والتجارب التقنية للتمكّن من إزالة أو تعطيل التقنيات التي تزيد من

---

102 Reynolds, and SM Irwin. “Tracking digital footprints,” Op.cit., p. 182.

103 Iwa Salami. "Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?", Studies in Conflict & Terrorism, Vol. 41.12, 2018, pp. 968-989, p. 985.

المجهولية الرقمية[104]، إلا أن الموقف السلبي المتّبع من قبل سلطات إنفاذ القانون لا يساهم من مجاراة أو تجاوز عقبتها التي تقيّد تنفيذ مهامهم.

ومن ميزة المجهولية الرقمية، سننتقل إلى ميزة التحويل النقدي التي تتصف بها العملات التشفيرية، هذه الميزة التي أخرجتها من عالم الافتراض المطلق.

المبحث الثاني: ميزة تحويل العملة التشفيرية من وإلى نقود رسمية

تُعد النقود الرسمية **Fiat Currency** وسيلة الدفع الطاغية عالمياً نظراً لأنها مدعومة من قبل المصارف المركزية ومنظمة عبر القوانين، وتلقائياً يسهل تحويلها أو استبدالها فيما بينها.

وفي السياق نفسه، ما يميّز العملات التشفيرية عن التجارب الأولية لابتكار عملات رقمية هي امكانية استبدالها مع نقود رسمية. أي تطبيقياً، هناك امكانية تحويل أو استبدال عملة البيتكوين مثلاً إلى الدولار الأمريكي والعكس صحيح، تماماً مثلما تُستبدل الليرة اللبنانية بالدولار الأميركي.

تتمتع إذاً العملات التشفيرية بميزة التحويل من وإلى نقود رسمية، هذا على عكس بعض العملات الافتراضية غير التشفيرية. استحدثت هذه الميزة جسراً يربط بين العملات التشفيرية الكائنة في العالم الافتراضي مع العالم الواقعي المادي، فهناك تفاعل مباشر مع القطاع المالي والاقتصادي وذلك بعكس بعض العملات الرقمية الافتراضية غير القابلة للاستبدال التي تبقى في خانة "العالم الافتراضي غير الحقيقي"، وذلك نظراً لاقتصار مفعولها ونطاق استعمالها في الفضاء السيبراني.

---

[104] أجريت تجارب عديدة منها التي فصلت المستخدمين مؤقتاً عن برنامج طور، بحيث تُرك هؤلاء دون غطاء المجهولية خصوصاً لناحية إمكانية تحديد عنوان بروتوكول الإنترنت IP الخاص.

–Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. "Deanonymisation of clients in Bitcoin P2P network." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2014.

في طبيعة الحال، تخضع وسائل التحويل أو الاستبدال فيما بين النقود الرسمية إلى الأنظمة والقواعد المرعية وبعضها تتطلب الترخيص المسبق وتخضع لرقابة المؤسسات المالية، في وقت تقع أغلبية وسائل التحويل من وإلى العملات التشفيرية خارج نطاق القوانين، فلا تستحصل الجهات المعنية على التراخيص ولا تخضع إلى الرقابة... ولكن سرعان ما باشرت تتبدل الأوضاع مع البدء بإخضاع بعض من هذه الوسائل إلى الأنظمة المالية وقواعد مكافحة تبييض الأموال الإلكترونية وتمويل الإرهاب، وذلك سواء من قبل المنظمات الإقليمية أو السلطات التشريعية المحلية.

من أهم طرق التحويل في سياق العملات التشفيرية نذكر أولاً عملية الشراء المباشر من البائع عبر منصات النظير للنظير **P2P**، ثانياً أجهزة الصراف الآلي الخاصة الـ **ATM**، وثالثاً منصات التبادل الإلكترونية **Exchanges**. نعطي لمحة سريعة عن كل واحدة على انفراد:

<u>أولاً. عملية الشراء المباشر عبر منصات النظير للنظير Peer to Peer Platform:</u>

يمكن شراء عملة تشفيرية مباشرة من البائع عبر لقائه شخصياً وتسمى بعملية **Cash in Person**، بحيث يدفع الشاري نقداً ما يعادل قيمة العملة التشفيرية التي يريدها ويرسل البائع بدوره الرصيد المتفق عليه إلى عنوان أو محفظة الشاري. يتعرّف الشاري على البائع عبر مواقع إلكترونية تسمى بمنصات النظير للنظير **Peer to Peer Platform** التي توفر نظام وساطة، تربط بمن يرغب ببيع عملاته التشفيرية بالراغبين بشرائها، فيتم التواصل واللقاء تبعاً.

إن هذه الطريقة فيما لو اتّخذ الشاري الحذر، تُعدّ الأكثر أماناً وصوناً للمجهولية الرقمية ولهوية الفرقاء، فلا مشاركة هنا لأية بيانات تعريفية ولا أي أثر رقمي لعملية التحويل... إلا أن وسيلة التبادل هذه محصورة في النطاق المحلي، الأمر الذي قد يعتبره البعض بالمقيّد ويدفعهم باللجوء إلى طرق تمكّنهم من عبور الحدود إلكترونياً.

توفر منصات النظير للنظير وسائل تحويل أخرى على غرار وسيلة التحويل النقدي المباشر **Cash in Person**، تتمثل بالدفع الإلكتروني وإيداع المشتري النقود مباشرة في الحساب المصرفي للبائع.

تُعتبر منصة **Localbitcoins.com** الفنلندية المؤسسة في العام 2012، أشهر منصة **P2P** التي توفر خدمات التحويل المذكورة أعلاه. ولكن، امتثالاً للتشريعات الفنلندية والأوروبية كالتنظيم الأوروبي العام لحماية البيانات الـ **GDPR** [105] والتوجيهات والقوانين التي ترعى مكافحة تبييض الأموال وأبرزها الـ **AMLD**، اشترطت وتطلّبت هذه المنصة في العام 2018 من مستخدميها إبراز وإثبات هوياتهم الشخصية عند إجراء بعض العمليات، وفي شهر حزيران من العام 2019 حجبت وألغت من دون سابق إنذار، ميزة التحويل عبر اللقاء المباشر بين المشتري والبائع، ولقد أعلنت عن هذا الإجراء عبر حسابها الرسمي على موقع تويتر[106].

LocalBitcoins.com Buy bitcoins Sell bitcoins Post a trade Help ▾ Sign up free Log in

Sell bitcoins online in Lebanon

Buyer	Payment method	Price / BTC	Limits	
hamza72 (3000+; 98%)	Cash deposit: BBAC bob omt pay cash in europe	14,238,422.00 LBP	1,500,000 - 30,000,000 LBP	Sell
NaderALDirany (100+; 96%)	Cash deposit: ✳⚡ CASH✓ OMT✓ BOB✓ Audi Online✓ ⚡✳	11,246,294.80 LBP	At least 200000 LBP	Sell
NaZziXx (500+; 100%)	Cash deposit: Cash in Person-OMT-BOB Min 500$ Max 30K$ 70803804	10,451,732.46 LBP	750,000 - 75,000,000 LBP	Sell
ggg666 (30+; 98%)	Cash deposit: OMT or cash max $100k 70612903	15,202,957.42 LBP	50,000 - 150,000,000 LBP	Sell

Show more... ▾

3. صورة لموقع **Local Bitcoins** يبيّن عرض وطلب البيتكوين في لبنان بمطلع عام 2020.

---

105 General Data Protection Regulation
– Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation), **Official Journal of the European Union**, L.119/1, 4 May 2016.

106 https://twitter.com/LocalBitcoins/status/1135872083962081281

لم يرحّب العديد بخطوة منصة **Localbitcoins.com**، فلجأ الكثر إلى منصات **P2P** أخرى توفر الخدمات عينها، نذكر منها **local.bitcoin.com** و **hodlhodl.com** و **bisq.network**. ونستنتج أنه لطالما لا تنظيم وتشريع موحّد وإلزامي يشمل جميع هذه المنصات، سيكون البديل دوماً جاهزاً أمام الراغبين لاستبدال المنصات التي تمتثل مع القوانين.

ثانياً. أجهزة الصراف الآلي الخاصة:

في عصر التكنولوجيا المالية **FinTech** والتحوّل الرقمي في القطاع المصرفي، اشتدّ التنافس فيما بين المصارف لتقديم وتوفير كافة خدماتها إلكترونياً عبر شبكة الإنترنت والتطبيقات الإلكترونية، وعمدت إلى تسهيل التعامل مع العملاء من خلال توفير خدمات مختلفة عبر أجهزة الصراف الآلي **ATM** [107]. ونظراً لأهمية أجهزة الصراف الآلي التي تسمح للعميل بإجراء العديد من العمليات المصرفية على مدار الساعة دون الحاجة للدخول إلى المصرف واللجوء إلى موظفيه، بدأت تنتشر أجهزة الصراف الآلي الخاصة بالعملات التشفيرية.

لجهة آلية عمل جهاز الصراف الآلي الخاص بالعملات التشفيرية، فهي تعمل بشكل مماثل لأجهزة الصراف الآلي التابعة للمصارف ولكن مع بعض أوجه الاختلاف. تمكّن هذه الأجهزة من شراء وبيع أو بالأحرى استبدال العملات التشفيرية بالنقود الرسمية، وهي متصلة مباشرة بشبكة الإنترنت على عكس الأجهزة التابعة للمصارف، وبدلاً من إدخال بطاقة ائتمان للحصول على النقود، يمكن إيداع النقود في الآلة لاستحصال رصيد من عملة تشفيرية معينة، يتم إرساله مباشرةً إلى محفظة المستخدم الخاصة.

إن هذه الأجهزة تُجيز إرسال وتحويل العملات التشفيرية بسرعة فائقة وإلى أي مكان في العالم مقابل اقتطاع مبلغ رمزي. إلا أن ما يجذب الكثير ومنهم المجرمين، هو مقدرة شراء والاستحواذ على جهاز

[107] Automated Teller Machine

صراف آلي من أيٍّ كان وبكل بساطة، على عكس الإجراءات المطوّلة والشروط المطلوبة من قبل المؤسسات المالية التي ترغب بوضع جهاز صراف آلي.

فبهذه الطريقة، وبمبلغ مالي شبه بسيط يمكن لمن يشاء أن يقتني الصراف الآلي الخاص به والذي يمكّنه من شراء العملات التشفيرية بالنقود الرسمية، وأنه عبر تسديد مبالغ إضافية[108]، يمكن شراء صراف آلي ذات الميزة المزدوجة والتي تقدّم خاصية تحويل النقود إلى عملات تشفيرية والعملات التشفيرية إلى نقود. بحسب موقع **BTC Coin ATM Radar**، هناك حالياً قرابة الـ 6391 صراف آلي منتشر في 73 دولة[109].

من الملاحظ بأن هذه الأجهزة قائمة بشكل مستقل عن أي جهة رسمية أو مصرف أو مؤسسة مالية مرخصة، وهذا أمر خطير بحد ذاته، فلا من رقابة مسبقة عبر استحصال التراخيص والموافقة المسبقة من المصرف المركزي ولا رقابة لاحقة تتأكّد من حسن الامتثال للقوانين والانظمة المرعية. ونظراً لانتشار أجهزة الصراف الآلي أكثر فأكثر، عمدت بعض الدول إلى وضع أسس وتنظيم قانوني لها، بحيث أضحت تمنح التراخيص لشرائها وتثبيتها وتشغيلها، وألزمت العملاء على ابراز وثائق رسمية أو بيانات شخصية تعرّف وتكشف عن هوياتهم مثل إبراز دفتر القيادة[110] عند الرغبة في إتمام أي عملية؛ ولكن في المقابل، تبقى العديد من هذه الأجهزة خارج نطاق القوانين وليست بحد ذاتها مبرمجة للتثبّت من هوية العملاء، خصوصاً إذا ما كانت المبالغ المحوّلة غير كبيرة، مما يعني إضفاء طابع المجهولية على هذه العمليات.

ثالثاً. منصات التداول Exchanges:

منصات التداول هي مواقع إلكترونية توفر خدمات شراء وتبادل العملات التشفيرية على أنواعها. توفر معظم المنصات خدمة التبادل فيما بين العملات التشفيرية أي مثلاً بين عملة البيتكوين والإثيريوم

---

[108] يقدّر سعر جهاز الصراف الآلي الذي يحوّل ويستبدل النقود الرسمية إلى العملات التشفيرية بحوالي 6500 د.أ. وإن اضافة ميزة استبدال العملات التشفيرية إلى نقود رسمية (أي يوفر الجهاز الخدمة المزدوجة) يكلّف قرابة الـ 5500 د.أ.

[109] https://coinatmradar.com/

[110] وهذه إجراءات بدأت تُتبع في كندا والولايات المتحدة الأميركية.

Ethereum (مختصر **ETH**)، في حين توفر بعض المنصات الأخرى خدمة التبادل فيما بين العملات التشفيرية بين بعضها ومع النقود الرسمية مثلاً فيما بين عملة البيتكوين والدولار الأميركي.

على الراغب بالاستفادة من خدمات منصة معينة، أن يتسجّل ويفتح حساباً على الموقع. من أشهر منصات التداول نذكر منصة **Binance** [111] اليابانية و **Coinbase** [112] و **Kraken** [113] الأميركيتان. تعمد التشريعات الحديثة على تعداد العملات التشفيرية تحت خانة العملات الافتراضية أو الأصول الافتراضية لإضفاء الطابع "الخيالي" وغير الجدي عليها، توصلاً لتثبيط الجمهور من اعتمادها كوسيلة دفع، طبعاً لأن مصلحتها تكمن بإبقاء السيطرة المالية المفروضة من قبل المصارف المنظمة قانوناً.

نحن لا نتوافق مع الجهات الرسمية والتشريعات التي تعمد إلى إدراج العملات التشفيرية في خانة العملات الافتراضية غير القابلة للتحويل وحصر آلية تحويلها، وذلك كمحاولة لإبعاد الخطر عن أنظمة الدفع المالية التقليدية ولسلب مفعول هذه العملات وتأثيرها على العالم الواقعي. إن ميزة التحويل النقدي هي من إحدى العوامل التي جعلت من العملات التشفيرية رائجة ومعتمدة سواء من قبل المواطن العادي أو كبار التجار والشركات العابرة للحدود وحتى المجرمين، وميّزتها عن العملات الافتراضية غير القابلة للتحويل والمجرّدة من أي مفعول أو فرصة جدية تمكّنها من مد جسر إلى الاقتصاد والتعاملات المالية. فلطالما بقيت النقود الرسمية هي وسيلة الدفع الوحيدة المقبولة والمنظمة عالمياً، ستبقى العملات التشفيرية وسيلة خطرة بيد المجرمين لتحويل ونقل أموال. وعليه، سنعالج في الباب الثاني أبرز المخاطر الناتجة عن العملات التشفيرية وارتكاس الأنظمة التشريعية على هذه المخاطر.

---

[111] https://www.binance.com/en

[112] https://www.coinbase.com/

[113] https://www.kraken.com/

الباب الثاني: تَبعة المفاعيل التطبيقية للعملات التشفيرية

قرابة شهر حزيران من العام 2011، لحظ عملاء منصة **MT. Gox** (كانت 80% من عمليات البيتكوين تجري عبرها) من نقص في أرصدتهم من عملة البيتكوين، تبين لاحقاً بأن مقرصناً نجح من الولوج إلى نظام المنصة وسرقة كمية كبيرة من العملات المحفوظة في حسابات العملاء. بعد فترة وجيزة، طُرحت كميات من هذه العملات إلى البيع بأسعار بخسة وزهيدة، مما نتج إلى هبوط قيمة البيتكوين من حوالي 17 دولار أميركي إلى بضع سنتات فقط. لم تقتصر الخسائر بالماديات فقط، بل سرعان ما تسربت البيانات الشخصية للعملاء إلى العلن، الأمر الذي بيّن النطاق الواسع للخرق السيبراني الذي تعرضت له المنصة.

بيّن هذا الخرق خطورة النضوج السريع لهكذا تقنية، وبلورت طبيعة البيتكوين المتقلبة وإشكالية الثقة بهذا النظام اللامركزي... هذا النظام غير المنظّم قانوناً والذي أصبح عالماً متاحاً أمام الجميع، والذي بدأ يطرح مخاطر عديدة من عدة أوجه.

كان الخرق لأكبر منصة (آنذاك) تأثيراً مباشر على البيتكوين، فما قبل هذا الخرق لم يكن كما بعده، فهذا الخرق أسر انتباه المشرع خصوصاً بتغلغل آثاره إلى مجالات وفروع قانونية عديدة، فكان الحل الوحيد هو التحّرك والحد من "لا قانونية" عالم العملات التشفيرية.

وعليه، سنبحث في الفصل الأول المخاطر الناتجة عن العملات التشفيرية لننتقل في الفصل الثاني لمعالجة أبرز التطبيقات القانونية في معالجة هذه العملات.

الفصل الأول: المخاطر الناتجة عن العملات التشفيرية

تُلحق العملات التشفيرية مخاطر على مستثمريها ومستخدميها لا بل تتخطى نطاق المتعاملين معها وصولاً إلى الاقتصاد والأمن المالي والرقمي. بشكل عام، تنقسم هذه المخاطر إلى عدة فئات مترابطة مع بعضها البعض، فمنها الاقتصادية، ومنها الأمنية والتقنية ومنها القانونية، فلا يوجد إطار قانوني واضح ينظمها ويحكم تعاملاتها.

لذا، سنعالج المخاطر الملحقة بالتعامل بالعملات التشفيرية في المبحثين التاليين:

المبحث الأول: المخاطر التقنية والاقتصادية

المبحث الثاني: المخاطر الناتجة عن التحديات القانونية

المبحث الأول: المخاطر التقنية والاقتصادية

تلعب الطبيعة اللامركزية لدى العملات التشفيرية دوراً أكثر من بارز في عالم الاقتصاد والأعمال، ولكن هذا الدور قد يشكّل تحدّ سلبي للاقتصاد العالمي والسياسة المالية، فلا من دولة تسيطر عليها ولا من جهة تنظمها.

مع ذلك، لا يمكن تجاهل واقعة إحداث ورقة البيتكوين البيضاء ثورةً في عالم التكنولوجيا... فيعتبر أوليغ ستراتييف **Oleg Stratiev** [114] أنها ساهمت من تحسين حوكمة الشركات، وأعادت تقنية البلوكشاين تشكيل المشهد المالي، بحيث خلقت منافسة إضافية توجّه نحو أنظمة لامركزية، متيحةً للمستهلك المزيد من الخيارات وساحة مفتوحة أمام الشركات الأكثر جدارة، وأنها عززت أيضاً الكفاءة والثقة والشفافية والابتكار من كافة النواحي.

[114] Oleg Stratiev. “Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand." Banking & Finance Law Review, Vol. 33.2, 2018, pp. 173-212, pp. 211,212.

ولكن في المقابل، ليس من الممكن إنكار المخاطر الناتجة أو المحتملة سواء من طبيعة العملات التشفيرية وتفاعلها في عالم الاقتصاد والمال، أو من آلية عمل التكنولوجيا القائمة عليها.

أولاً. المخاطر الاقتصادية الراهنة والمحتملة:

يرى بريان إها **Brian Eha** أن عملة البيتكوين تشكل تهديداً ثلاثياً للأسواق القائمة، وذلك لإمكانية عملها كمخزن للقيمة مثل الذهب؛ كوسيلة للدفع في التجارة الإلكترونية مثل بايبال **Paypal**، وكشبكة معاملات عالمية مثل ويسترن يونيون **Western Union** [115].

وباعتقاد آخرين[116]، للعملات التشفيرية القدرة بأن تشكّل تحدّ جدي للمصارف المركزية، خصوصاً إذا ما بدأت تؤثّر على العرض النقدي وبالتالي على السياسة المالية والنقدية ككل، وذلك طبعاً بمنأى عن اتصافها بمقوّمات النقود. ولا شك بأن التقنيات الحديثة القائمة عليها هذه العملات ساهمت من جعلها كتلة اقتصادية هائلة ذات قوة[117]، فهناك حالياً قرابة الـ 2035 عملة تشفيرية تتخطى قيمتها السوقية **Market Cap** [118] الـ 220 مليار دولار أمريكي[119].

ولكن للمصرف المركزي الأوروبي **ECB** رأي معاكس. فبموجب ورقة منشورة في شهر أيار من العام 2019، استقصت فرضية تأليف العملات التشفيرية (الأصول التشفيرية) في الوقت الراهن خطراً على

---

115 Brian Patrick Eha. **How Money Got Free: Bitcoin and the Fight for the Future of Finance**, Oneworld Publications, 2017, p. 5.

116 Antoine Bouveret and Vikram Haksar. "What Are Cryptocurrencies? A Potential New Form of Money Offers Benefits While PosingRisks," **Money, Transformed The Future of Currency in a Digital World**, International Monetary Fund, June 2018, p. 27, www.imf.org

117 ماريلين أورديكيان، "العملات الافتراضية المشفّرة في الحقل الجنائي السيبراني"، مجلة الدفاع الوطني، العدد 108، نيسان 2019، الصفحات 73-105، ص. 80، https://www.lebarmy.gov.lb/ar/content/108-d

118 Market Capitalisation (Market Cap) أي الرسملة السوقية، تعني القيمة السوقية لجميع الأسهم القائمة لشركة معينة. يتم احتسابها بضرب سعر السهم السوقي بالعدد الإجمالي للأسهم القائمة.

119 https://coinmarketcap.com/all/views/all/, Accessed 18 Oct. 2019.

الاستقرار المالي ضمن المنطقة الأوروبية[120]. علماً أن تجارب بعض الدول ذات الاقتصاد المنهار والوضع المالي المتأزّم مثل فنزويلا ولبنان، قد برهنت بأن عملة البيتكوين هي بديل استثنائي لعملاء المصارف والمواطنين وبأنها توفّر مهرباً لهؤلاء من سيطرة المصارف على أموالهم[121].

– **<u>الطبيعة المُتَقَلِّبة Volatile:</u>**

في نطاقٍ أضيق، تواجه العملات التشفيرية وبالأخص البيتكوين من مشكلة التقلّب وعدم استقرار قيمتها **Volatility** [122]، فالتقلبات التي تشهدها البيتكوين أكثر بكثير من تلك الذهب والعملات الوطنية. من الصحيح بأن العملات الوطنية تشهد أيضاً تقلبات مماثلة، ولكن تتولّد هذه العقبة أثناء حلقات تضخم مفرطة، والتي عادةً تتوج "بموت" العملة[123]. وفي حين شهدت حدّة هذه التقلبات انخفاضاً خلال عامي 2016 و2017، بحيث توقّع العديد من المحللين الاقتصاديين آنذاك أن يستمر التدني مع نضوج الشبكة، إنما تضخّم هذا التقلب أكثر فأكثر وبشكل حادّ في نهاية عام 2017 وبداية عام 2018[124]، حيث سجل سعر البيتكوين في 17 كانون الأول من العام 2017 أعلى درجاته حوالي 19,000 دولار أميركي وسرعان ما انخفض إلى 13,800 دولار أميركي بعد خمسة أيام فقط. فكنتيجة، كثر توصيف عملة البيتكوين "بالفقاعة" **Bubble** وانطرحت مسألة انعدام الثقة بها خصوصاً كوسيلة للتبادل والدفع... فكيف لتاجرٍ مثلاً

[120] European Central Bank Crypto-Assets Task Force. Paper on **Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures**, No. 223, May 2019, p. 22, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

[121] Graham Smith. “Lebanon Fights for Separation of Money and State as Residents Use Bitcoin to Evade Capital Control.” Bitcoin.com, 27 Feb. 2020, www.news.bitcoin.com, Accessed 28 Feb. 2020.

[122] Girasa Rosario. **Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives**, Springer, 2018, p. 15.

[123] Saifedean Ammous. "Can Bitcoin’s Volatility Be Tamed?", The Journal of Structured Finance, Vol. 24.1, 2018, pp. 53-60, pp. 57,58.

[124] id. p. 56.

أن يسعّر بضاعته بالبيتكوين، إذا ما كان سعر هذه السلعة في اليوم الأول 10 دولار أميركي وفي اليوم الثاني 20 دولار؟[125]

إن هذا القدر من التقلّب خطير جداً، وبالأخص على المستثمرين. فكثر هم من أقدموا على صرف عملاتهم التشفيرية بسعر صرف منخفضة، لتعود وتضاعف قيمتها بعد بضعة أيام أو أسابيع، والعكس صحيح. ولعل أبرز مثال يمكن أن نذكره للإضاءة على الموضوع، ما حصل مع لازلو هانيكز **Laszlo Hanyecz** الملقّب برجل البيتزا، فهذا الأخير كان وراء أول عملية دفع بعملة البيتكون خلال شهر أيار من العام 2010، بحيث أقدم على شراء البيتزا (عدد 2) لقاء 10.000 بيتكوين من مطعم بابا جونز بيتزا **Papa John's Pizzas**. فآنذاك سعر العملة الواحدة لم تتخطى البضع سنتات، ولقد تحولت هذه البيتزا إلى الأغلى في العالم بحيث تبلغ قيمتها بتاريخ كتابتنا لهذا المبحث[126] حوالي 85 مليون دولار أميركي.

أما سبب هذه التقلبات فهي عديدة، نذكر منها:

– العملات التشفيرية ليست مدعومة بعملة رسمية أو من قبل سلطة شرعية،

– الأخبار السيئة حولها كالخطط المتجهة نحو منعها أو حظرها من قبل السلطات المعنية، أو شهر إفلاس منصات تبادل كبيرة مثل MT. Gox.

– مستقبلها الغامض والمبهم خصوصاً حيال تصنيفها كنقود أو سلع إلخ.

– التفريغ الفجائي لأعداد هائلة من هذه العملات في السوق وبأسعار منخفضة، أي زيادة نسبة العرض من دون زيادة في نسبة الطلب.

– التلاعب بالأسعار

– الخروقات الأمنية بدورها تهدد الثقة الممنوحة للعملات التشفيرية، وهذا ما سنبحثه أدناه.

[125] Felix Salmon. “The Bitcoin Bubble and the Future of Currency,” Medium, 3 Apr. 2013, https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb, Accessed 27 Aug. 2019.

[126] الواقع في 24 أيلول من العام 2019.

ثانياً. المخاطر الأمنية والهجمات السيبرانية:

نظام البيتكوين بحد ذاته هو نظام آمن[127]، أي غير قابل للقرصنة، ولكن هذا لا يعني أن البيتكوين وسائر العملات التشفيرية محمية من القرصنة والاختراق والسرقة وسائر أنواع الهجمات السيبرانية.

ففي البداية، عندما نتحدث عن سرقة عملة تشفيرية كالبيتكوين، نكون في نطاق كشف المفتاح الخاص التابع لمحفظة صاحب العملة. مما يعني أنه بافتقار هذا المفتاح، لا مجال للدخول إلى المحفظة وبالتالي الاستيلاء على العملة، وذلك نتيجة التقنية القائمة عليها البيتكوين والمغايرة لتلك التي تقوم عليها بطاقات الائتمان، والتي تستوجب الكشف عن بيانات سرية عند إجراء تحويل أو عملية مصرفية[128].

على مدار السنين، اقتُرفت عمليات السرقة بشتى الطرق والوسائل كالتصيّد الإلكتروني **Phishing**، فمثلًا سُرق مبلغ 50 مليون دولار أميركي من موقع **Blockchain.info** الذي يُعدّ من أبرز المواقع التي توفّر خدمة المحفظات الإلكترونية، وذلك عن طريق إدراج إعلانات خادعة ومضللة على محرّك غوغل[129].

أما الطريقة الثانية الأكثر شيوعاً، تتجلّى بقرصنة منصات التداول وخرق أمنها وصولاً إلى سرقة العملات. بحسب وكالة الأنباء رويترز، فلقد بلغ عدد البيتكوين المسروق من منصات التداول ابتداءً من العام 2011 لحين مطلع العام 2018 الـ 980,000 بيتكويناً، مقابل استرجاع عدد ضئيل منها فقط[130]

[127] Jonathan B. Turpin. "Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework." Indiana Journal of Global Legal Studies, Vol. 21, 2014, pp. 335-368, pp. 339,340.

[128] Mauro Conti, et al. "A Survey on Security and Privacy Issues of Bitcoin." IEEE Communications Surveys & Tutorials, Vol. 20.4, 2018, pp. 3416-3452, p. 3423.

[129] ماريلين أورديكيان، "العملات الافتراضية المشفّرة في الحقل الجنائي السيبراني"، ص. 85.

[130] Jemima Kelly, and Tommy Wilkes. “Exclusive: Coincheck Hackers Trying to Move Stolen Cryptocurrency-Executive,” Reuters, 30 Jan. 2018, https://www.reuters.com/article/us-japan-cryptocurrency-cybercrime/exclusive-coincheck-hackers-trying-to-move-stolen-cryptocurrency-executive-idUSKBN1FJ28Y, Accessed 23 Aug. 2019.

والوتيرة فقط إلى الارتفاع[131]. من أول وأكبر عمليات الخرق والسرقة نذكر تلك التي استهدفت منصة **MT. Gox** اليابانية، ولقد كانت الخسائر فادحة نتيجة لإجراء 80 بالمئة من عمليات التحويل لعملة البيتكوين آنذاك عبرها. قدّرت الخسائر بنصف مليار دولار، الأمر الذي أدى إلى إعلان افلاس المنصة وتدهور سعر البيتكوين بين ليلة وضحاها.

أما في لبنان، وقع العديد من مالكي العملات التشفيرية ضحية عمليات الاحتيال والسرقة الدولية، إلا أن ما شهده البلاد خلال شهر تشرين الأول من العام 2019، هو لربما أول عملية سرقة لعملات لبنانيين من قبل جهات من المرجّح بأنها لبنانية. فخلال ثورة السابع عشر من تشرين الأول، في حين كان اللبنانيين يقودون ثورة أشعلها الوضع الاقتصادي المتردي والنظام المصرفي، خُرق جدار الحماية **SS7 Firewall** التابع لشركة الاتصالات تاتش **Touch**. وكنتيجة تعرّض الكثر إلى عمليات تبديل بطاقات السِم **Sim Card** والتي تُعتبر نوع من أنواع هجمات سرقة الهوية **Identity Theft**. منح هذا الهجوم الجهة المقرصنة إمكانية التحكم برقم الجهة المستهدفة عبر إقناع مقدم الخدمة لتبديل الرقم إلى بطاقة سِم

[131] 1. مثال: في شهر كانون الثاني من العام 2018، تمّت سرقة ما يقارب الـ 523 مليون دولار أميركي من منصة التبادل اليابانية الشهيرة Coincheck بعد تعرّضها للقرصنة من قبل مجهولين.

-يراجع:

-BBC News. “Coincheck: World's biggest ever digital currency 'theft',” bbc.com, 27 Jan. 2018, https://www.bbc.com/news/world-asia-42845505, Accessed 23 Aug. 2019.

2. مثال: في شهر آب من العام 2016، تعرّضت منصة BitFinex الشهيرة إلى القرصنة وخسرت ما يقارب الـ 120000 بيتكوين.

-يراجع:

-Mauro Conti, et al. "A Survey on Security and Privacy Issues of Bitcoin." Op.cit., p. 3434.

خاضعة لسيطرة المقرصن، فأدّت الهجمة إلى سرقة ما يُقارب 30،000 دولار أميركي من العملات التشفيرية[132].

بشكل عام، أثارت طبيعة هذه السرقة مسائل قانونية وصعوبة لدى القضاء عند تطبيق النصوص الخاصة بجريمة السرقة، خصوصاً بأنها تتضمن الكشف غير المصرّح به للمفتاح الخاص والذي بدوره لا قيمة له[133]. ارتابت سلطات الملاحقة الشكوك حول مدى إمكانية الملاحقة والتحقيق بعمليات السرقة هذه في ظل اعتبار البعض بأن هذه العملات ليست بعملات أو نقود ذات قيمة وبأن النصوص التقليدية غير قابلة للتكييف من قبل القضاء، فهل هو قرصنة وولوج غير مشروع وخرق أمني أم سرقة أو تعدٍّ على بيانات؟

– **خسارة المفتاح الخاص هي خسارة أبدية:**

يمتلك مستخدمو البيتكوين مفاتيح تسمح لهم بإثبات ملكية البيتكوين على الشبكة، فباستخدام هذه المفاتيح يستحوذون على الحق بإنفاقها وتوقيع المعاملات وتحويلها إلى مالك (عنوان) جديد. غالباً ما يتم تخزين المفاتيح في محفظة رقمية على جهاز الحاسوب أو الهاتف الذكي أو على برنامج[134] أو جهاز مستقل يأخذ شكل الناقل التسلسلي العام **Universal Serial Bus (USB)**[135]. تكمن أهمية امتلاك

---

132 Aro.steem. " Lebanese Crypto-currencies Stolen Users-sms Attack," steempeak.com, November 2019, https://steempeak.com/@aro.steem/crypto-stolen-users-lebanese-telecom-touch-ss7-firewall-has-been-breached?fbclid=iwar1eddn4jei3ynpta56lfkz0pw3l0gnh4a_e9jueg41qdmbomvvp6kk2ywm, Accessed 6 Dec. 2019.

133 Gregory Bischoping. "Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016." University of Pennsylvania Law Review, Vol. 167, 2018, pp. 239-259, p.243.

134 وتسمى المحافظ الساخنة Hot Wallets.

135 وتسمى المحافظ أو الحافظ البارد Cold Storage.

المفتاح الخاص الذي يمّكن من توقيع معاملة ما، بأنه الشرط المسبق الوحيد لإنفاق البيتكوين، فهذا المفتاح يمنح كل مستخدم سلطة التحكم المطلق بالعملات الكائنة في المحفظة.[136]

إن خسارة أو نسيان أو ضياع المفتاح الخاص تعتبر من المخاطر الأمنية وإحدى سلبيات نظام العملات التشفيرية. ففقدان المفتاح الخاص يعني فقدان المالك لعملاته التشفيرية[137]، وذلك لأن حيازة المفتاح الخاص هو بمثابة حيازة عدد طائل من الأوراق النقدية أو سبائك من المعادن الثمينة، فبفقدانها أو نسيان مكانها أو تعرضها للسرقة تعني خسارتها وعدم قدرة استرجاعها[138]، فمن هذه الناحية هي ليست إطلاقاً مثل كلمات المرور ليتمكن المرء من إعادة تعيينها والحصول على كلمة أو رمز سري جديد.

برهنت الأحداث بأن هذه الميزة تغلغلت إلى نطاق قانون الإرث ومفاعيل انتقال الذمة المالية، بحيث حُرم كثر من وراثة أموال طائلة جراء عدم معرفتهم أو عدم كشف المتوفي لمفتاحه الخاص، والذي بوفاته نقل عملاته التشفيرية معه إلى الحياة الأبدية... وهذا ما حصل مع منصة تبادل العملات التشفيرية **QuadrigaCX** بحيث توفي مؤسسها بشكل مفاجئ، وتبين أنه كان الوحيد الذي يستحوذ على المفتاح الخاص للمحفظة، مما أدى إلى فقدان حوالي 145 مليون دولار أميركي[139].

تكمن أهمية هذه المخاطر بأنها تنتج عنها مخاطر قانونية فالعلاقة فيما بينها قائمة ومترابطة، لذلك كان من الضروري التهيئة للمخاطر القانونية الناتجة عنها.

---

136 Andreas M. Antonopoulos. **Mastering Bitcoin: Programming The Open Blockchain**, "O'Reilly Media, Inc.", 2nd edition, 2017, p. 1.

137 Arvind Narayanan, et al. **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**, Princeton University Press, 2016, p. 117

138 Antonopoulos. **Mastering Bitcoin: Programming The Open Blockchain**, Op.cit., p.269.

139 Doug Alexander. “Crypto CEO Holding Only Passwords That Can Unlock Millions in Customer Coins,” Bloomberg, 4 Feb. 2019, https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem, Accessed 14 Nov. 2019.

المبحث الثاني: المخاطر الناتجة عن التحديات القانونية

تنبثق إشكاليات قانونية عديدة جراء التبني الواسع للعملات التشفيرية وتقنية البلوكشاين. تنطرح أبرز هذه الصعوبات والعوائق في نطاق القانون المدني خصوصاً في مجال حماية المستهلك والقانون الجزائي، بحيث تعاني السلطات التشريعية والسلطات القضائية أينما كان من التأقلم مع التحديات التي تثيرها هذه التقنيات الحديثة، التي ينبغي معالجتها.

أولاً. التحديات التي تواجه القانون المدني وحماية المستهلك:

بشكل عام، إن البيتكوين والعملات التشفيرية هي أموال رقمية ذات قيمة معينة وقابلة للتداول والتحويل والتملّك، فتمنح مالكها حقوقاً معينة... من هنا ندخل بإيجاز إلى القانون المدني، خصوصاً لجهة حماية المستهلك المنغمس في العالم الاقتصادي الرقمي.

من مميزات نظام البيتكوين والعملات التشفيرية القائمة على البلوكشاين أن العمليات القائمة عليها هي نهائية، أي لا رجوع عنها **Irreversible** [140]. فمن أرسل مثلاً مقداراً معيناً من البيتكوين إلى عنوان محدد، لا يمكنه إذا ما غيّر رأيه أن يعود عن قراره ويلغي التحويل الذي أجراه، وهذه الميزة مستنبطة من واقعة انعدام سلطة مركزية تتحكم أو تشرف على العمليات المالية.

تتبلور سلبيات ومخاطر هذه الميزة عند تعرّض صاحب العملات إلى السرقة أو إذا تم خداعه أو بكل بساطة إذا ما أرسل من دون قصد العملات إلى العنوان الخاطئ، فما من جهة معينة يمكن التواصل

---

[140] Sarah Meiklejohn, et al. "A fistful of bitcoins: characterizing payments among men with no names," *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 127-140, p. 127.

معها لتسوية الوضع. كنتيجة، يغدو الحائز على العملة هو صاحب السلطة، مما يستعصي ويعقّد الوصول إلى هذه الأموال واسترجاعها؛ حتى عن طريق القضاء[141]، إلا إذا وافق الحائز الجديد على ردها...

ما سبب عجز القضاء أو العوائق في هكذا حال؟ في بادئ الأمر، على المحكمة الكشف عن هوية الشخص الذي بحوزته هذه العملات المسروقة أو المرسلة إليه عن طريق الخطأ إلخ، مما يعني تطلّب إزالة السرية عن بعض البيانات والمعلومات الخاصة. ثانياً، هناك احتمال كبير بأن هذا الحائز الجديد غير الشرعي موجود في دولة أخرى، فأصبحنا أمام تنازع صلاحيات قضائية. وأخيراً، من السهل جداً إنشاء عناوين عامة وحسابات جديدة تُنقل إليها العملات، فيتم تضليل المسار الرقمي للعملة، وبالتالي تُعاق إمكانية التعقّب.

هذا من جهة... من جهة ثانية، إن العملات التشفيرية كما رأينا هي متقلبة الأسعار، مما يعرّض مستثمريها والمستهلك إلى خسائر فادحة، طبعاً من دون أي وسيلة تمكّن هؤلاء من استرجاع ما خسروه... فلا تعويض قانوني. ولهذا السبب، تُحذّر أغلبية المؤسسات المالية والسلطات التشريعية من هذه المخاطر والتقلّب بالأسعار.

إن غياب الطرق والإمكانية القانونية للتعويض عن العملات الضائعة أو المسروقة أو المسلوبة، تعتبر من نقاط ضعف العملات التشفيرية ومن أبرز المخاطر المحيطة بها. فكم من منصة تداول تعرّضت للسرقة ولم يتمكن عملائها من استرجاع أموالهم، وكم من هذه المنصات أو المشاريع تبيّنت أنها وهمية، نجحت من الاحتيال على زبائنها، بعد إيهامهم ودفعهم بتسليم أموالهم بهدف الاستثمار بمشاريع تبيّنت في وقت لاحق بأنها وهمية...

[141] Rhys Bollen. “The legal status of online currencies: are Bitcoins the future?”, Journal of Banking and Finance Law and Practice, Vol. 24.4, December 2013, p. 283, https://ssrn.com/abstract=2285247

ثانياً. التحديات الناتجة عن العرض الأولي لعملة ICO:

ظهر العرض الأولي لعملة **Initial coin offerings** أو **ICO**، مؤخراً كمشروع بديل شعبي للتمويل الجماعي **Crowdfunding**. بهذه الطريقة الحديثة، تجمع الفئة الريادية بالأعمال رأس مال الشركة أو المشروع الجديد عبر عملية طرح وبيع أولية لـ"الرموز" **Tokens**، والتي تمنح مالكها الحق في استخدام المنتج أو الخدمة التي ستطورها[142]. تحوّلت الـ **ICO** في العام 2017، إلى الطريقة الرائدة عالمياً للتمويل خصوصاً لدى الشركات الناشئة **Startups** [143]. اكتسحت الـ **ICO** عالم ريادة الأعمال والتجارة الدولية والإلكترونية، وشكّلت نوعاً ووسيلة حديثة للتمويل، بحيث تهافت أصحاب رؤوس الأموال إلى تأسيس شركات تطرح عملات تشفيرية. قُدّرت الأموال المجموعة من قبل هذه الشركات في العام 2017 بـ 5 مليار دولار أميركي، ولقد حصدت شركة **Tezos** لوحدها مبلغ 230 مليون دولار و**Filecoin** قرابة 200 مليون دولار[144].

تجلّت خطورة الـ **ICO** بأنها وسيلة غير منظّمة **Unregulated** [145]، تُجمع من خلالها الأموال من الجمهور مقابل منحهم عملتهم الخاصة، كما هو الحال عند طرح شركة معينة لأسهما للاكتتاب. من

---

[142] Jiasun Li, and William Mann. "Initial Coin Offerings and Platform Building," 2018 WFA, 2019 AFA, p. 2, https://ssrn.com/abstract=3088726

[143] Katalyse.io. "How Cryptocurrency is Disrupting the Global Economy," Medium, 10 Jan. 2018,
https://medium.com/the-mission/how-cryptocurrency-is-disrupting-the-global-economy-89347581aa93, Accessed 11 May 2018.

[144] CB Insights. "Blockchain Startups Absorbed 5X More Capital Via ICOs Than Equity Financings In 2017," cbinsights.com, 18 Jan. 2018,
https://www.cbinsights.com/research/?s=Blockchain+Startups+Absorbed+5X+More+Capital+Via+ICOs+Than+Equity+Financings+In+2017

[145] بدأت بعض الدول باتخاذ الإجراءات التنظيمية والقانونية حيال هذه المشاريع، إلا أنه خلال العام 2017 عندما وصل نضوج هذه المشاريع إلى ذروته، كانت الدول تفتقر إلى أية قوانين أو إجراءات تنظّم المشاريع وترشد وتحمي المستثمرين، الأمر الذي ساهم من انتشار المشاريع الوهمية والكاذبة.

هذا المنطلق، يستحوذ المستثمر على الـ **Token** (بمعنى العملة) الخاصة بتلك الـ **ICO**، ولدى إطلاق المشروع رسمياً من قبل الشركة، يحصل المستثمر على نسبة أرباح، بالإضافة إلى حق وامكانية التداول بها واستعمالها لشراء السلع والخدمات عبر شبكة الإنترنت. لجأ العديد إلى الـ **ICO** لتفادي العراقيل والصعوبات التي تترافق مع عملية استقطاب التمويل المناسب والإجراءات القانونية والمصرفية الصارمة عند التقدم بطلبات التسجيل والقروض[146]. نود الإشارة إلى أنه يمكن شراء هذه العملات أو الرموز بالنقود الرسمية والعملات التشفيرية مثل البيتكوين أو الإثيريوم[147].

كثرت الشكوك حول شرعية ومصداقية شركات الـ **ICO**، فتبين أنّ أغلبيتها وهمية تهدف إلى استحواذ المال عن طريق المشاريع الاحتيالية... ونظراً لطبيعتها العالمية، تخطّت تداعياتها السلبية الحدود الجغرافية كافةً وتضاعفت نتائجها وضحاياها. ففي النهاية، إن أكثرية هذه الشركات هي عبارة عن منصات إلكترونية، تستقطب أموال الجمهور لقاء منحهم عملات رمزية ذات قيمة وهمية وغير مستقرة مجرّدة من أية ضمانات. ولقد حذّرت السلطات الأميركية[148] كما الأوروبية[149] من مخاطر التعامل مع الـ **ICO**، مشيرةً إلى وقوعها خارج النطاق القانوني الشرعي، على غرار انعدام سبل حماية المستهلكين والمستثمرين.

---

146 Salomon Fiedler, et al. Study requested by the European Parliament's Economic and Monetary Affairs Committee (ECON), on "**Virtual Currencies**," No. PE 619.016, Brussels, 2018, p. 13.

147 Arjun Kharpal. "Tokenization: The World of ICO's," CNBC, 16 Jul. 2018, https://www.cnbc.com/2018/07/13/initial-coin-offering-ico-what-are-they-how-do-they-work.html, Accessed 23 Sep. 2018.

148 https://www.sec.gov/ICO

149 The European Securities and Markets Authority-ESMA. Statement: "ESMA Highlights ICO Risks for Investors and Firms," 13 Nov. 2018, https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms

ولعله كان المشترع الفرنسي من السباقين الذين عمدوا إلى تنظيم الـ **ICO** بموجب قانون **PACTE** [150]، بحيث تنص المادة 85 منه[151] على حرية تقدم الجهات المعنية بالـ **ICO** للحصول على تأشيرة أو ترخيص اختياري **(Visa)** من هيئة الأسواق المالية الفرنسية **Autorité des Marchés Financiers (AMF)** لتقديم طرح أولي لعملة أو ما سموه بالرمز **Token**. عند درس طلبات الترخيص، ستُقدم الـ **AMF** من التأكد من مدى توافق وتطابق مضمون الطلب مع نصوص قانون **PACTE**. أما الـ **ICO** التي تفتقر إلى التأشيرة فلن يتم حظرها، إلا أنها ستخضع لقيود في مجال التسويق. استقطبت هذه الشركات المحتالين الذين جعلوا من الـ **ICO** وسيلتهم الجديدة للاستيلاء على أموال الجمهور، ولعل أبرز الوسائل تجلّت بمخطط بونزي **Ponzi Scheme** [152] وبعملية "الضخ والتفريغ" [153] **Pump and Dump** [154]. تعتبر عملية النصب الأشهر في عالم العملات التشفيرية تلك التي ارتكبتها **Bitconnect** عبر مخطط البونزي، فهذه الأخيرة استقطبت آلاف المستثمرين وبلغت قيمتها السوقية حوالي 2.7 مليار

---

[150] LOI No. 2019-486 du 22 Mai 2019 relative à la croissance et la transformation des entreprises (1), JORF No. 0119 du 23 Mai 2019, texte No. 2. https://www.legifrance.gouv.fr/eli/loi/2019/5/22/ECOT1810669L/jo/texte

[151] art. 85: "art. L. 552-4.-Préalablement à toute offre au public de jetons, les émetteurs peuvent solliciter un visa de l'Autorité des marchés financiers."

[152] مخطط البونزي عبارة عن عملية إستثمار إحتيالية، تعمل عن طريق الدفع للمستثمرين القدامة الأرباح عبر الأموال والاستثمارات المستحصلة من مستثمرين جدد، موهمين إياهم أن مصدر هذه الأرباح ناتجة عن استثماراتهم.

-راجع في هذا السياق:

-Stafford C. Baum. **Cryptocurrency Fraud: A Look into the Frontier of Fraud**, *University Honors Program Theses*, 2018, p. 4, https://digitalcommons.georgiasouthern.edu/honors-theses/375

[153] تُقترف عملية "الضخ والتفريغ" عبر إقدام المعنيين على نشر الأخبار والتصاريح الكاذبة والمعلومات المضللة إلى الأسواق والبورصة، بهدف رفع قيمة أسهمهم (أو في الحالة الراهنة، العملات التشفيرية)، وعند التوصل إلى القيمة المرغوبة، يباشرون ببيع كميات هائلة من هذه الأسهم لدرجة أن قيمتها تعود وتنخفض وتلحق الأضرار بسائر المستثمرين.

-راجع في هذا السياق:

-U.S. Securities and Exchange Commission. "Pump and Dump Schemes," March 2001, https://www.sec.gov/fast-answers/answerspumpdumphtm.html

[154] Stafford C. Baum. **Cryptocurrency Fraud: A Look into the Frontier of Fraud**, Loc.cit.

دولار أميركي، وذلك عبر الإعلان عن مخططات وهمية تتوعد المستثمرين بعوائد خيالية وفوائد تصل إلى 0.25% في اليوم الواحد ومن دون أية مخاطر. ففي السابع من شهر كانون الأول من العام 2018، كان سعر عملة **Bitconnect** (المعروفة بالـ **BCC**) 432 دولار أميركي، ولكن بعد حوالي الأسبوع وبالتحديد في الخامس عشر هبط سعرها بشكل مفاجئ إلى 290 دولار أميركي... تبين لاحقاً بأن المعنيين كانوا يصفّون عملاتهم لأنهم كانوا على علم مسبق بإعلان إقفال الشركة في السادس عشر، بحيث استدرك الجميع بواقعة تعرضهم للاحتيال، فهبطت قيمة العملة بعد ثلاثة أيام إلى25.91 دولار أميركي[155]. يتم حالياً ملاحقة الشركة بعدة دعاوى ومن قبل أكثر من جهة ودولة[156].

على غرار **Bitconnect**، هناك عدد لا يحصى من العمليات الاحتيالية التي ترتكب. هنا، من الجدير ذكر دور هيئة الأوراق المالية والبورصات الأمريكية **SEC**، التي تعمل مؤخراً جاهدةً إلى ملاحقة هؤلاء وتغريمهم الملايين[157]، ولعل من أبرز الجهات التي تقوم على ملاحقتها هي الـ **REcoin** و**DRC**[158] **World** و **Kik Interactive Inc** [159]. فعلى أي أساس وأي قانون تتم هذه الملاحقات؟ ومن أي منظار قانوني تتم معالجة العملات التشفيرية؟

---

155 Tom Alford. “Bitconnect Scam: The $2.6 BN Ponzi Scheme [2019 Update],” TotalCrypto.io, 8 Oct. 2018, https://totalcrypto.io/bitconnect-scam/

156 See, IN RE BITCONNECT SECURITIES LITIGATION, *Wildes et al. v. BitConnect Trading Ltd. et al.,* No.9:2018cv80086, http://securities.stanford.edu/filings-documents/1064/B00_01/201873_r01c_18CV80086.pdf

157 See, *Securities and Exchange Commission v. PlexCorps, Dominic Lacroix, and Sabrina Paradis-Royer*, No. 1:17-cv-07007-CBA-RML (E.D.N.Y. 2 Oct. 2019)

158 U.S. The Securities and Exchange Commission. “SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds,” 29 Sept. 2017, https://www.sec.gov/news/press-release/2017-185-0

159 U.S. The Securities and Exchange Commission. “SEC Charges Issuer With Conducting $100 Million Unregistered ICO,” 4 Jun. 2019, https://www.sec.gov/news/press-release/2019-87

الفصل الثاني: التطبيقات القانونية لتنظيم العملات التشفيرية

بعد التطور السريع في سوق العملات التشفيرية وازدياد التعامل معها مواكبةً لارتفاع قيمتها السوقية والمالية، كان لا بدّ من المشرّع سواء الدولي أو المحلي أن يخرج عن صمته ويتخذ موقفاً حيالها.

تنوّعت المواقف واختلفت المقاربات في وقت أضحى نهج السكوت مضرّاً أكثر مما هو فعّال، فاستبق بعض المشرعين المبادرة التي لا مهرب منها عاجلاً أم آجلاً. ففي حين اكتفى البعض بتوجيه الإنذار، بادر البعض إلى الحظر التام بالتعامل بالعملات التشفيرية، أما آخرين فعمدوا إلى تشريعها سواء بتعديل قوانينهم الموجودة أو عبر سن تشريعات جديدة.

وعليه، سنبحث في المبحث الأول موقف أبرز الجهات الدولية لننتقل في المبحث الثاني للتداول ببعض المواقف الداخلية.

المبحث الأول: الموقف الدولي والإقليمي

اختلفت المواقف التي تبنّتها المنظمات والجهات الرسمية الدولية حيال العملات التشفيرية واختلفت مقارباتها وآلية التعامل معها، فيستوجب البحث بأهم هذه المواقف.

أولاً. موقف المصرف المركزي الأوروبي ECB:

بدأ المصرف المركزي الأوروبي من استكشاف "العملات الافتراضية" في العام 2011، ونشر تقريره الأول عنها في العام 2012 تحت عنوان "مخططات العملات الافتراضية" "**Virtual Currency Schemes**"[160]، تلاه تقرير ثانٍ في العام 2015 [161]. جرّاء ازدياد الاهتمام العالمي في السنوات الأخيرة،

---

[160] ECB. **Virtual Currency Schemes**, October 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[161] ECB. **Virtual Currency Schemes**, February 2015, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

أنشأ المصرف المركزي الأوروبي فرقة عمل داخلية سُميّت بالـ **Crypto-Assets Task Force**، تختص بتطوير مفهوم العملات الافتراضية وتقييم تأثيرها المحتمل على بعض مجالات مسؤوليتها الأساسية كالسياسة النقدية والاستقرار المالي والمدفوعات والبنية التحتية للسوق. ولقد أصدرت هذه الفرقة أول ورقة لها في شهر أيار من العام 2019 [162]، وبخطوتها الأولى تبنّت مصطلح "الأصول التشفيرية" **Crypto-Assets** وحصرت نطاق بحثها فقط بالعملات التشفيرية دون غيرها من العملات الرقمية الافتراضية[163]. تخلص الورقة إلى أن الأصول التشفيرية يمكن إدارتها بموجب الإطار القانوني والتنظيمي الحالي؛ وهذا موقف لافت، خصوصاً أن الغالبية تتجه إلى ضرورة سن تشريعات جديدة، ولكن بالطبع مع الأخذ بعين الاعتبار امكانية تغيير هذا التقييم في المستقبل مع استمرار تطور سوق العملات التشفيرية.

من جهة أخرى، يرى المصرف المركزي الأوروبي على أن الأصول التشفيرية ليست لها قيمة جوهرية، ولا تدخل في عداد أي فئة من فئات التوصيف التقليدية، وأن قيمتها مستنبطة من التعامل بها وقناعة أصحابها بقيمتها. يدرك المصرف أيضاً أن الأصول التشفيرية يمكن أن تشكل خطراً عندما يتعلق الأمر بتبييض الأموال وتمويل الإرهاب وحماية المستهلك، ولكن مع ذلك، اعترف بفوائد تقنية البلوكشاين المحتملة لدى النظام المالي.

ثانياً. مجموعة العمل المالي FATF:

في شهر حزيران من العام 2019 ، تبنّت مجموعة العمل المالي **FATF** إرشادات[164] حديثة تُعنى "بالأصول الافتراضية" **Virtual Assets** (مختصر **VA**) ومقدمي هذه الخدمات" **Virtual Asset**

---

162 European Central Bank Crypto-Assets Task Force. Paper on **Crypto-Assets**, Op.cit., p. 3,

163 ibid.

164 FATF. “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

Service Providers (مختصر **VASPs**)، بالإضافة إلى مذكرة تفسيرية للتوصية رقم 15 [165] توضح كيفية تطبيق متطلباتها فيما يتعلق بالأصول الافتراضية ومقدمي خدمات الأصول الافتراضية، لا سيما في ما يتعلق بتطبيق النهج القائم على المخاطر **Risk-Based Approach**[166] في أنشطة أو عمليات الأصول الافتراضية ومقدمي خدمات الأصول الافتراضية، وذلك بهدف مكافحة تبييض الأموال و تمويل الإرهاب. تجدر الإشارة إلى أن هذه الوثيقة أدخلت تحديثات بمضمون الإرشادات المنشورة في العام 2015 والتي سبق وناقشناها[167].

تحثّ مجموعة العمل المالي السلطات التشريعية على ضرورة اتخاذ خطوات قانونية وعملية على وجه السرعة، لمنع إساءة استخدام الأصول الافتراضية. ويشمل ذلك تقييم وفهم المخاطر المرتبطة بالأصول الافتراضية ضمن نطاق صلاحياتهم القانونية والقضائية، وتطبيق قوانين مكافحة تبييض الأموال وتمويل الإرهاب قائمة على المخاطر، على مقدمي خدمات الأصول الافتراضية وتحديد الأنظمة الفعالة لإجراء المراقبة أو الإشراف على هؤلاء.

---

[165] FATF. "International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation-The FATF Recommendations," June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[166] النهج القائم على المخاطر يعني أن تقوم الدول والسلطات المختصة والمصارف بتحديد وتقييم وفهم مخاطر تبييض الأموال وتمويل الإرهاب، واتخاذ التدابير المناسبة وفقاً لهذه المخاطر.

[167] See FATF. "Guidance for a Risk Based Approach: Virtual Currencies," France, June 2015, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

ذكرنا مسبقاً بأنه في شهر تشرين الأول من العام 2018، تبنت وعرّفت المجموعة مصطلحي "الأصول الافتراضية" و"مقدمي خدمات الأصول الافتراضية"[168] بحيث وسعت نطاقها لتشمل منصات التبادل والتداول كافة[169] (أي تلك التي تقوم بالتحويلات فيما بين العملات التشفيرية والنقود الرسمية بالإضافة إلى التحويلات القائمة فيما بين العملات التشفيرية[170])، ومقدمي الخدمات المالية للـ **ICOs** ومقدمي خدمات المحفظات إلخ.[171]

لغايات تطبيق توصياتها، أوصت المجموعة على ضرورة تطرق الدول إلى الأصول الافتراضية على أنها "أموال" **propert**y أو "عائدات/إيرادات "**proceeds** أو "أموال" أو موارد مالية أو أصول أخرى" أو ذات قيمة أخرى[172]. وأنه ينبغي على الدول أن تطبق التدابير المناسبة لتتماشى مع توصياتها بشأن الأصول الافتراضية ومقدمي خدمات الأصول الافتراضية. ولقد فرضت التعديلات الجديدة على مقدمي الخدمات الاستحصال على ترخيص أو التسجيل في مكان ممارسة نشاطها، وإذا ما كانت ترغب بمد هذا النشاط إلى نطاق سلطة دول أخرى، فعليها أن تستحصل على ترخيص من السلطات المختصة لدى هذه الدول أيضاً[173].

---

[168] FATF. “Regulation of Virtual Assets,” France, 19 Oct. 2018, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/regulation-virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

[169] FATF. “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” 2019, p. 8.

[170] وذلك على عكس التوجيه الأوروبي الخامس لمكافحة تبييض الأموال AMLD 5 الذي حصر نطاق تطبيقه بالمنصات التي تُعنى بالتحويلات فيما بين العملات التشفيرية والنقود الرسمية.

[171] FATF. “Regulation of Virtual Assets,” 2018, Loc.cit.

[172] Paragraph 1 of the Interpretative Note to Recommendation

[173] Par. 3 of the Interpretative Note to Recommendation 15, “International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation-The FATF Recommendations,” Loc.cit.

ثالثاً. صندوق النقد الدولي:

أضاء صندوق النقد الدولي على مميزات العملات التشفيرية وتطرّق إلى التطور التكنولوجي السريع في عالم التجارة ومدى تأثيرها على سرعة إتمام الصفقات. ولقد صرّحت المديرة العامة للصندوق النقد الدولي السيدة كريستين لاغارد بأن النقود ذات الطبيعة المتغيرة وأن الإقبال على النقود الورقية يتراجع، فعلى المصارف المركزية أن تدرس إمكانية إصدار عملة رقمية، بحيث قد يكون للدولة دور في توفير النقود للاقتصاد الرقمي[174]. وفي تصريح آخر أعربت "لاغارد" بأن العملات التشفيرية والتكنولوجيا "المُزعزعة" **Disruptive Technology** "تهزّ" الانظمة المالية ويجب مراقبتها للحفاظ على الاستقرار، بالاضافة إلى المواكبة التشريعية[175].

لقد نشر صندوق النقد الدولي ورقة بحثية[176] تتناول ايجابيات وسلبيات العملات الرقمية الصادرة عن المصارف المركزية. ولقد اعتُبر بأنه يمكن لهذه العملات أن تعزز الشمول المالي **Financial Inclusion** والخصوصية والأمن في التحويلات المالية، وذلك لقاء رسوم زهيدة وآلية فعالة، ولكن حذّر من مخاطر تستهدف الاستقرار المالي.

---

174 Christine Lagarde. “Winds of Change: The Case for New Digital Currency,” International Monetary Fund, 14 Nov. 2018, https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency

175 Elizabeth Schulze. “Cryptocurrencies are ‘clearly shaking the system,’ IMF’s Lagarde says,” CNBC, 10 Apr. 2019, https://www.cnbc.com/2019/04/11/cryptocurrencies-fintech-clearly-shaking-the-system-imfs-lagarde.html, Accessed 29 Jul. 2019.

176 Tommaso Mancini Griffoli, et al. Paper on Casting Light on Central Bank Digital Currencies, International Monetary Fund, SDNEA2018008, 12 Nov. 2018, https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233

من جهة أخرى، أصدر الصندوق النقد الدولي في العام 2019 وبالتعاون مع البنك الدولي عملة "**Learning Coin**" الرقمية، التي لا تتمتع بأي قيمة نقدية ومتاحة فقط للعاملين في المؤسستين الدوليتين. تتمثل أهداف هذا المشروع بمساعدة موظفي هذه المنظمات على اكتساب بعض الخبرة العملية مع تقنية البلوكشاين، ولتطوير مفهوم العملات التشفيرية بشكل أفضل لدى هؤلاء، على غرار مفاهيم أخرى كالعقود الذكية **Smart Contracts**، وتطبيقاتها المحتملة لأغراض غير قانونية مثل تبييض الأموال[177].

رابعاً. التوجيه الأوروبي الخامس لمكافحة تبييض الأموال AMLD5:

دخل التوجيه الأوروبي الخامس لمكافحة تبييض الأموال **Anti-Money Laundering Directive** (مختصر **AMLD5**) رقم 2018/843 [178] حيّز التنفيذ بتاريخ 9 تموز من العام 2018 بعدما أدخل تعديلات مهمة على التوجيه الرابع. مُنحت الدول الأعضاء فترة انتقال لحين شهر كانون الثاني من العام 2020، بهدف تعديل قوانينها المحلية لتصبح متجانسة مع أحكام التوجيه. ما ميّز هذا التوجيه بأنه الأول من نوعه على صعيد الاتحاد الأوروبي وذلك لتناوله العملات التشفيرية والرقمية الافتراضية على أنواعها.

في الأسباب الموجبة، استدرك المشرع الأوروبي عدم خضوع مقدمي خدمات المحفظة **Custodian Wallet Providers** (مختصر **CWP**) ومنصات العملات الافتراضية **Virtual**

---

[177] Landon Manning. “IMF and World Bank Launch 'Learning Coin' to Explore Cryptocurrency,” Nasdaq, 15 May 2019, https://www.nasdaq.com/articles/imf-and-world-bank-launch-learning-coin-explore-cryptocurrency-2019-05-15, Accessed 28 Jul. 2019.

[178] Council of Europe: Directive 843/2018 of the European Parliament and of the Council of 30 May 2018 amending Directive 849/2018 on the prevention of the use of financial system for the purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, **Official Journal of the European Union**, L.156, 19 Jun. 2018.

Currency Exchange (مختصر **VCE**) لموجب كشف الحركات المشبوهة ضمن نطاقها، وبالتالي ركّز على امكانية استغلال الجماعات الإرهابية هذا الأمر لنقل الأموال عبر الأنظمة المالية أو عبر شبكات العملات التشفيرية، وذلك من خلال إخفاء العمليات أو الاستفادة من درجات معينة من المجهولية التي توفرها هذه الخدمات. بهدف مكافحة عمليات تبييض الأموال وتمويل الإرهاب، وُجدت الضرورة لتغطية التوجيه الخامس مقدمي خدمات المحفظة ومنصات العملات الافتراضية لتمكين السلطات من مراقبة عمليات العملات التشفيرية المذكورة.

وبالفعل، أدخل التوجيه ولأول مرة مصطلح وتعريف عبارتي "العملات الافتراضية" (تمت مناقشتها مسبقاً) ومقدمي خدمات المحفظة **CWP** بموجب المادة 1 فقرة 2 (د)(19)[179] بحيث قصد وضع تعريف واسع للعملات الافتراضية وتجنّب تصنيفها، مشيراً إلى أنها تستخدم في الوقت الراهن كوسيلة دفع ويمكن أن تستعمل كوسيلة للتبادل **Means of Exchange** ومخزن للقيمة**Store of Value** والاستثمار...[180]

في حين عرف مقدمي خدمات المحفظة على أنه "هيئة تقدّم خدمات تحمي المفاتيح الخاصة التشفيرية بالنيابة عن المستخدم، على غرار خدمات تخزين ونقل العملات الافتراضية"[181]. إن هذا التعريف يعني أن مقدمي الخدمات الذين لا يحتازون على المفاتيح الخاصة كشركتي **Trezor** و **Ledger Nano S** تقدمان خدمات **Hardware Wallets**) لا يخضعون إلى أحكام التوجيه.

---

[179] عدلت المادة 1 أحكام المادة 3 من التوجيه الأوروبي الرابع لمكافحة تبييض الأموال Anti-Money Laundering Directive (AMLD 4) رقم 2015/849.

[180] AMLD 5 recital (10).

[181] Art. 1 (2) (d)(19) of AMLD 5 states: “custodian wallet provider” means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.”

في المقابل، لم يعرّف المشرع الأوروبي مصطلح منصات العملات الافتراضية **VCE**، حاصراً إياها في سياق الصك فقط بتلك التي تُعنى بالتحويل فيما بين النقود الرسمية **Fiat Currency** والعملات الافتراضية، مستبعداً من أحكامه التحويلات فيما بين العملات الافتراضية، بالإضافة إلى عمليات التبادل عبر مواقع النظير للنظير **P2P**[182].

ولقد فرضت المادة 44 (فقرة 29) على مقدمي خدمات المحفظة ومنصات العملات الافتراضية شرط التسجيل أو الترخيص الاجباري، في حين مُنحت الجهات والمؤسسات التي تقع خارج نطاق التوجيه، الحق بالتسجيل الاختياري.

ومن المنظار الدولي، ننتقل إلى أبرز المقاربات في القوانين الوضعية.

المبحث الثاني: الموقف الداخلي

انبثقت في السنوات الماضية ثلاث مقاربات لجهة التعامل مع العملات التشفيرية على الصعيد التشريعي والقانوني. ففي حين اختارت بعض الدول سلوك حظر ومنع العملات التشفيرية على مستوى مطلق أو جزئي، فضّلت دولاً أخرى التريّث ودراسة مقاربات دول أخرى (مع تحذير الجمهور من المخاطر المحتملة) وهذا ما يعرف بنهج الـ **Wait and See**. أما الفئة الأخيرة، فانتقت طريق التشريع والتنظيم،

182 Tom Keatinge, et al. Study commissioned by European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, on "**Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses: Counter-terrorism**," No. PE 604.970, May 2018, pp. 38-42.

سواء عبر فرض الضرائب أو إخضاع العملات التشفيرية إلى أحكام قوانين تبييض الأموال وتمويل الإرهاب أو إلى القوانين المالية إلخ. فسنستعرض أدناه المواقف المتباينة المتبعة من قبل بعض الدول:

أولاً. كندا:

تجيز كندا استعمال واستخدام العملات التشفيرية والرقمية على أنواعها. وبحسب صفحة الويب التابعة "للوكالة الكندية للمستهلك المالي" **Financial Consumer Agency**، فإنه من المسموح "استخدام العملات الرقمية (**Digital Currencies**) لشراء السلع والخدمات على شبكة الإنترنت وفي المتاجر التي تتقبلها. يمكن أيضاً شراء وبيع العملات الرقمية عبر المنصات المفتوحة، التي يطلق عليها تسمية منصات العملات الرقمية أو التشفيرية."[183]

اعتبرت "وكالة الإيرادات الكندية" **CRA** [184] أن "العملات الرقمية" هي سلعة، وبالتالي إن استخدامها لشراء السلع والخدمات تعتبر بمثابة صفقة مقايضة. وعليه، تخضع عمليات العملات الرقمية إلى الضريبة[185]. أما لناحية الوضع القانوني لهذه العملات، فسنداً لقانون العملة الكندي **Currency Act**، فإنها ليست بالعملة الرسمية **Legal Tender**، لأن الدولار الكندي هو العملة الرسمية في البلاد[186].

---

[183] Financial Consumer Agency of Canada. “Digital Curency,” 2018, https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html#toc0, Accessed 3 Aug. 2019.

[184] Canada Revenue Agency

[185] Al-Shikarchy (Mariam), et al. “Canadian Taxation of Cryptocurrency … So Far,” Gowling WLG, *Lexology*, 14 Nov. 2017, https://www.lexology.com/library/, Accessed 19 Sept. 2019.

[186] Canadian Currency Act, R.S.C., 1985, c. C-52, paragraphs 7 and 8, https://laws-lois.justice.gc.ca/eng/acts/c-52/FullText.html

نشير إلى أن كندا هي أول دولة عالجت العملات الرقمية في قوانينها[187] وذلك عبر اخضاعها لأحكام قانون مكافحة تبييض الأموال وتمويل الإرهاب الكندي[188] [189].

ثانياً. الجمهورية الفدرالية الألمانية:

أقرت ألمانيا التعامل مع البيتكوين وسائر أنواع العملات التشفيرية والافتراضية، بحيث تُعتبر بحسب هيئة الرقابة المالية الفيدرالية الألمانية **BaFin** [190] وحدةً للقياس **Unit of Account** وبالتالي أداةً مالية **Financial Instrument** [191]. فليست بالعملة الرسمية **Legal Tender** ولا تقع في عداد النقود الإلكترونية **e-money** [192].

وفي العام 2018، نشرت وزارة المالية الألمانية دليلاً يعالج مدى خضوع البيتكوين وسائر العملات الافتراضية للضرائب، ولقد وضّحت بأن استعمال هذه العملات كوسيلة دفع هي معفاة من الضرائب[193].

---

187 Christine Duhaime. "Canada Implements World's First National Bitcoin Law," DUHAIME LAW, 22 Jun. 2014, https://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/, Accessed 19 Sept. 2019.

188 Bill C-31, An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures, Second Session, Forty-first Parliament, 62-63 Elizabeth II, 2013-2014, Statutes of Canada 2014 Ch. 20, https://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/third-reading

189 راجع الفصل الثاني من الباب الأول للقسم الثاني.

190 Bundesanstalt für Finanzdienstleistungsaufsicht

191 BaFin. "Virtual Currency (VC)," Federal Financial Supervisory Authority, https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html, Accessed 18 Sept. 2019.

192 Loc.cit.

193 German Federal Ministry of Finance (BMF). "VAT Treatment of Bitcoin and Other So-Called Virtual Currencies-ECJ Decision of October 2015, C-264/14, Hedqvist (BMF Letter)," 27 Feb. 2018, https://www.loc.gov/law/foreign-news/article/germany-federal-ministry-of-finance-publishes-guidance-on-vat-treatment-of-virtual-currencies/

ولكن إن التعامل المبني على أساس التجارة سواء لناحية اقتناء العملات أو بيعها أو شرائها، أو تقديم خدمات الوساطة الرئيسية عبر منصات التداول، تستوجب حصول ترخيص مسبق، وإن أي مخالفة في هذا النطاق معاقب عليه وفقاً للقسم 54 من القانون المصرفي الألماني **Kreditwesengesetz** [194].

ثالثاً. مملكة البحرين:

في شهر تموز من العام 2019، منح مصرف البحرين المركزي ترخيص "وحدة الأصول المشفرة" **(CRA)** لمنصة تداول "رين" **Rain** [195]، وبذلك أضحت هذه الأخيرة أول منصة عملات تشفيرية مرخصة في الشرق الأوسط... ولقد حصدت المنصة في جولتها الاستثمارية الأولى مبلغ 2.5 مليون دولار[196].

كانت المملكة البحرينية قد بدأت بتطبيق نهج "صندوق الرمل التنظيمي" [197] **Regulatory Sandbox** وكنتيجة، نشر المصرف المركزي التوجيهات النهائية الخاصة بعدة أنشطة ذات الصلة "بالأصول المشفرة"[198]. أوضح هذا البيان القواعد ومعايير الاشراف والانفاذ الخاص بهذه المنصات، واعتبر بأن الأصول المشفرة التي تعمل في ظل أنظمة البلوكشاين "جذبت الكثير من الاهتمام على مستوى العالم،

---

194 BaFin. “Virtual Currency (VC),” Loc.cit.

195 https://www.rain.bh/

196 https://blog.rain.bh/ar/rain-is-live-73t2wci9

197 نهج "صندوق الرمل التنظيمي" Regulatory Sandbox، عبارة عن مقاربة تنظيمية تسمح للشركات الخاصة والناشئة من امتحان واختبار الابتكارات، في بيئة مراقبة واستثنائية (إعفاءات خاصة، تمويل، وتسهيلات أخرى). يُجيز هذا النهج من مواكبة عصر التطور التكنولوجي السريع خصوصاً في الأسواق المالية (وظهور التكنولوجيا المالية المعروفة بـ FinTech أي Financial Technology)، بحيث يتم اختبار التقنيات الجديدة والخدمات مالية والأطر حديثة للأعمال، وذلك كمحاولة لمعالجة المعضلة بين رغبة القطاع الخاص في الابتكار ومحاولة المشرع بوضع إطار تنظيمي من دون حد الإبداع التقني.
-راجع في هذا السياق:

- Ivo Jenik, and Kate Lauer. Working paper on "Regulatory sandboxes and financial inclusion." Washington, DC: CGAP, 2017.

198 مصرف البحرين المركزي، "مصرف البحرين المركزي يصدر التوجيهات النهائية الخاصة بخصوص الأصول المشفرة ومنصات الأصول المشفرة"، 25 شباط 2019،

https://www.cbb.gov.bh/ar/media-center/مصرف-البحرين-المركزي-يصدر-التوجيهات-ا/

وتهدف قواعد مصرف البحرين المركزي إلى ضمان دخول الأنشطة ذات الصلة ضمن المحيط التنظيمي وتخضع لتدابير تنظيمية وإشرافية شاملة"[199].

رابعاً. الجمهورية الجزائرية الديمقراطية الشعبية:

فرض المشترع الجزائري حظراً تاماً بموجب المادة 117 من قانون المالية لسنة 2018 على عمليات شراء وبيع واستعمال وحيازة "العملات الافتراضية". ولقد عرّف مصطلح "العملات الافتراضية" على أنها "تلك التي يستعملها مستخدمو الإنترنت عبر شبكة الإنترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو بالبطاقة البنكية"[200]. لم تنص هذه المادة أو مواد أخرى من هذا القانون على عقوبة معينة تُفرض عند المخالفة، بل اكتفى المشترع الجزائري في الفقرة الأخيرة من المادة المذكورة بمعاقبة كل مخالفة طبقاً للقوانين والتنظيمات المعمول بها.

خامساً. الجمهورية الفرنسية:

منذ عام 2017، تبنت الحكومة الفرنسية والسلطات المعنية موقفاً ترحيبياً تجاه تقنية البلوكشاين. تم نشر العديد من التقارير الرسمية حول هذه التقنية والأصول الرقمية (كما سمّتها)، سواء من قبل الهيئات الحكومية[201] أو من قبل البرلمان[202]. وفي العام 2019، نُظّم بموجب قانون **PACTE** والنظام المرعي

---

[199] Loc.cit.

[200] قانون المالية الجزائري رقم 117-11، الجريدة الرسمية، عدد 76 تاريخ 28 كانون الأول 2017، ص. 54، https://www.joradp.dz/FTP/JO-ARABE/2017/A2017076.pdf

[201] Rapport au Ministre de l'Economie et des Finances, **Les crypto-monnaies**, 4 Juillet 2018,https://www.mindfintech.fr/files/documents/Etudes/Landau_rapport_cryptomonnaies_2018.pdf

[202] Office Parlementaire d'évaluation des Choix Scientifiques et Technologiques, **Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)**, 4 Juin 2018, https://www.senat.fr/rap/r17-584/r17-5841.pdf

لهيئة الأسواق المالية **Autorité des marchés financiers (AMF)** [203] الأصول الرقمية ومقدمي خدماتها.

تنصّ المادة 86 من قانون **PACTE**[204]، على مدى الزامية حصول مقدمي هذه الخدمات على الترخيص، بحيث حصرت موجب الاستحصال على الترخيص الإلزامي بفئتين فقط وهما، أولاً مقدمي خدمات حفظ الأصول الرقمية أو المفتاح المشفّر الخاص بالنيابة عن جهات ثالثة (بهدف حفظ أو تخزين أو تحويل الأصول الرقمية)، وثانياً مقدمي خدمات التحويل من وإلى نقود رسمية. يتم الاستحصال على هذا الترخيص من قبل الـ **AMF**، والتي لها سلطة قبول أو رفض الطلبات بحسب معايير محددة في نظامها. من أبرز هذه المعايير والشروط تلك الواردة في المادة 721-3، التي تنص على تقديم برنامج عمل مفصّل عن سنتين يتضمن النشاطات التي ينوي مقدم الخدمات على ممارستها، لائحة بأسماء الأصول الرقمية التي ستتعاطى معها، النطاق الجغرافي للخدمة إلخ[205].

وطبعاً، إن مقدمي خدمات الأصول الرقمية معرضين لعقوبات بحسب قانون **PACTE** في حال خالفوا أو لم يتقيدوا بالأصول والإجراءات المفروضة عليهم[206].

---

203 Règlement général de l'Autorité des marchés financiers, https://www.amf-france.org/eli/fr/aai/amf/rg/livre/7/20191219/notes/fr.html

204 art.86 (L. 54-10-4): “L'exercice de la profession de prestataire des services mentionnés aux 1 et 2 de l'article L. 54-10-2 est interdit à toute personne n'ayant pas été enregistrée au préalable par l'Autorité des marchés financiers.”

205 Aussi, Décret No. 2019-1213 du 21 Novembre 2019 relatif aux prestataires de services sur actifs numériques, JORF No. 0271 du 22 Novembre 2019, texte No. 25, https://www.legifrance.gouv.fr/eli/decret/2019/11/21/ECOT1919608D/jo/texte

206 Section 4 de l'article 86 de la loi PACTE.

سادساً. الجمهورية اللبنانية:

يُعتبر مصرف لبنان أول من حذّر في الشرق الأوسط من مخاطر العملات التشفيرية[207]، فموجب الإعلام رقم 900 تاريخ 19 كانون الأول من العام 2013 [208]، توجّه المصرف المركزي إلى المصارف والمؤسسات المالية ومؤسسات الصرافة ومؤسسات الوساطة المالية والجمهور ونبّههم مما سماه "النقود الافتراضية" وبالأخص البيتكوين. ولقد نص الاعلام على واقعة عدم خضوع "المنصات **(Platforms)** أو الشبكات **(Networks)** التي يتم بواسطتها اصدار وتداول هذه النقود" لأي تشريعات أو تنظيمات وعلى عدم وجود إطار حمائي قانوني يؤمن استرجاع الاموال التي تم بها شراء هذه النقود وفي حال تعرضت لخسائر. حذّر أيضاً من تقلب أسعار هذه العملات وواقعة تسهيلها للنشاطات الاجرامية خاصةً تبييض الاموال وتمويل الارهاب. استدراكاً لهذه المخاطر التي تم تعدادها في متن الإعلام، حذر مصرف لبنان شراء وحيازة واستعمال هكذا نقود.

في العام 2017، خلال المؤتمر السابع لشركة سي.أس.آر. ليبانون **The CSR 7th LEBANON FORUM** [209]، استدرك حاكم مصرف لبنان الأستاذ رياض سلامه بأن "العملات الإلكترونية" ستلعب دوراً بارزاً في المستقبل، ولكن أبدى بأنه "يتوجب على المصرف المركزي قبل ذلك أن يقوم بالتحضيرات اللازمة، وبالأخص استحداث أساليب الحماية من الجرائم الإلكترونية. فهيئة التحقيق الخاصة ولجنة الرقابة على المصارف تتعاونان لوضع نظام يمنع هذه السرقات." ولقد اعتبر الحاكم بأن

---

[207] Eric Barrier. “Lebanese central bank issues Middle East’s first Bitcoin warning,” Cointelegraph, 3 Jan. 2014, https://cointelegraph.com/news/lebanese_central_bank_issues_middle_east_s_first_bitcoin_warning, Accessed 3 Nov. 2018.

[208] مصرف لبنان، اعلام رقم 900 تاريخ 19 كانون الأول 2013 موجه للمصارف وللمؤسسات المالية ولمؤسسات الصرافة ولمؤسسات الوساطة المالية وللجمهور، https://www.bdl.gov.lb/news/more/5/111/65

[209] كلمة حاكم مصرف لبنان الأستاذ رياض سلامه خلال المؤتمر السابع لشركة سي.أس.آر. ليبانون **The 7th CSR Lebanon Forum**، في فندق فينيسيا، بيروت، 26 تشرين الأول 2017، http://www.bdl.gov.lb/news/more/8/250/251

العملات الإلكترونية هي سلع ترتفع وتنخفض أسعارها بلا مبرر وبالتالي ليست بعملة. ولكن المفاجئ بكلمة الحاكم هو اعتباره بان المصرف المركزي قد سبق ومنع "بشكل جازم استعمال الـ **Bitcoin** أو أي نوع آخر من العملات الإلكترونية، لأنها تشكل خطراً كبيراً على المستهلك وعلى أنظمة الدفع"، في حين لتاريخ القاء كلمته، كان الاعلام رقم 900 التحذيري هو المستند الرسمي الوحيد الذي تطرق إلى العملات الإلكترونية من هذه الناحية.

أصدرت هيئة الأسواق المالية في العام 2018، إعلاماً مماثلاً بعنوان "المخاطر المتعلقة بالنقود الإلكترونية" بحيث كررت في متنه محتوى الاعلام رقم 900 لجهة المخاطر، ولكن مع إضافة فقرة أولى، حظرت بموجبه "المؤسسات المرخصة إصدار النقود الإلكترونية Electronic Money " كما وحظرت على هذه المؤسسات فقط "من التسويق والتداول بالعملات الإلكترونية لحسابها أو لحساب عملائها بصورة مباشرة بما فيها المتداولة في الاسواق المالية المنظمة"[210].

من الواضح أن هنالك التباس وتناقض في المصطلحات المستخدمة في هذين الاعلامين خصوصاً الاعلام رقم 30 لعام 2018. فبضمن الاعلام المعنوَن بـ "المخاطر المتعلقة بالنقود الالكترونية"، ذُكرت ثلاث عبارات (من دون أي تعريف أو توضيح أو تفريق فيما بينها) وهي "النقود الإلكترونية **Electronic Money**" و"العملات الإلكترونية" و"النقود الافتراضية"... فنلاحظ عدم وحدة ودقة المصطلحات، ومن الجدير ذكره أن العملات التشفيرية أو كما سمته هيئة الاسواق المالية ومصرف لبنان بـ "النقود الافتراضية" و "العملات الالكترونية" ليست اطلاقاً بالنقود الإلكترونية **E-Money** التي تعتبر تمثيلاً رقمياً للنقود الرسمية، ولقد سبق وناقشنا هذا الأمر في الباب الأول. برأينا، لا تخضع العملات التشفيرية أو الرقمية

---

[210] هيئة الأسواق المالية، اعلام رقم 30 تاريخ 12 شباط 2018، الجريدة الرسمية، عدد 8 تاريخ 22 شباط 2018، ص. 1105 (المخاطر المتعلقة بالنقود الإلكترونية).

الافتراضية إلى الانظمة والقرارات التي ترعى النقود الإلكترونية **E–money**، وإننا نستغرب حشو عدة مصطلحات غير دقيقة من دون أي تفسير أو توضيح، مما يثير إرباك الجمهور والمؤسسات المعنية.

يمتد هذا الغموض إلى قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم 2018/81[211]. إذ تضمنت المادة الأولى منه تعريف عبارة "النقود الإلكترونية والرقمية"، وذلك على النحو الآتي:

"النقود الإلكترونية والرقمية (**Monnaie Électronique et numérique/Digital or Electronic Money**): هي وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية."

تكمن الإشكالية في عبارة "النقود الإلكترونية والرقمية"، وإذا ما كانت تتطرق في شقّها الأول أي "النقود الإلكترونية" إلى التعريف الصحيح لها كما نص عليها (مثلاً) التوجيه الأوروبي رقم 2009/110/EC[212]... وإذا ما كان الهدف عند إدراج عبارة "والرقمية" في الشق الثاني الدلالة إلى العملات التشفيرية والافتراضية على أنواعها كافة.

ففي البداية، إن مصطلح "النقود" ليس محبّذاً للإشارة إلى العملات التشفيرية، خصوصاً أن حاكم مصرف لبنان صرّح بأنها سلع وليست نقود[213]. وعلى غرار ذلك، إن التعريف بحد ذاته مبهم بعض الشيء وغير دقيق ولا ينطبق على العملات التشفيرية والرقمية الافتراضية.

---

[211] قانون رقم 81 تاريخ 2018/10/10، الجريدة الرسمية، عدد 45 تاريخ 2018/10/18، الصفحات 4546-4568 (قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي).

[212] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, **Official Journal of the European Union**, L.267/7, 10 Oct. 2009.

[213] كلمة حاكم مصرف لبنان الأستاذ رياض سلامه خلال المؤتمر السابع لشركة سي.أس.آر. ليبانون، مرجع سابق.

وفرضاً أنّ المشرّع أراد أن ينسب عبارة "النقود الإلكترونية والرقمية" فقط للعملات التشفيرية، فلِمَ تمّ لاحقاً التمييز بينهما في الفقرتين الرابعة والخامسة من المادة 116[214] عندما أورد عبارة "النقود الإلكترونية أو الرقمية"؟

بالإضافة إلى ذلك، وبعد أن أكّد حاكم مصرف لبنان مراراً على مشروعٍ لإصدار عملة رقمية محلية من قبل المصرف المركزي[215]، فهل ينطبق التعريف المذكور وأحكام القانون على هذه العملة بشكلٍ استباقي؟ في جميع الأحوال، وضعت المادة 61 [216] من هذا القانون مصير "النقود الإلكترونية والرقمية" بيد مصرف لبنان سواء لناحية تحديد ماهيتها وأنظمتها وطرق إصدارها على غرار استعمالها.

أما لناحية الشكل، نلاحظ ورود خطأ مادي بسيط في الترجمة الإنكليزية للفقرة الثامنة من المادة الأولى. ففي تعريف عبارة "النقود الإلكترونية والرقمية"، استُبدل حرف العطف الـ "**or**" بحرف العطف "**and**" فكانت النتيجة "**Digital or Electronic Money**" بدلاً من "**Digital and Electronic Money**".

---

[214] تنص المادة 116 على ما يلي:

"يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبالغرامة من عشرة ملايين إلى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين كل من: ...

4. قلد نقوداً الكترونية أو رقمية.

5. استعمل، مع علمه بالأمر، نقوداً الكترونية أو رقمية مقلدة."

[215] Brooke Anderson. “Salameh: Central Bank to Launch Digital Currency,” The Daily Star, 27 Oct. 2017, https://www.dailystar.com.lb/Business/Local/2017/Oct-27/424064-salameh-central-bank-to-launch-digital-currency.ashx

[216] تنص المادة 61 على ما يلي:

"تحدد الأنظمة الصادرة عن مصرف لبنان ماهية النقود الإلكترونية والرقمية وكيفية إصدارها واستعمالها والتقنيات والأنظمة التي ترعاها."

- نشير إلى أنّ المادة 64 تكرّر بدورها مضمون المادة 61 ولو بطريقة غير مباشرة: "...لمصرف لبنان حق إصدار الأنظمة اللازمة المتعلقة بالقواعد المنصوص عليها في هذا الفصل، لا سيما لجهة تنظيم أوامر الدفع والنقود الإلكترونية والرقمية والتحاويل والشيكات الإلكترونية والصورة الرقمية للشيك والتمثيل الرقمي للشيك والشيك الرقمي، وكيفية إصدارها واستعمالها، وأصول حفظ القيود المصرفية ومدة حفظها بالإضافة إلى وسائل الحماية والأمان اللازمة."

وبالتالي، نستنتج أنّ القانون اللبناني رقم 2018/81 أتى مبهماً وغير دقيق لناحية مفهوم النقود الإلكترونية والعملات التشفيرية. فإذا كان المقصود في هذا القانون العملات التشفيرية، فلِمَ استُعملت عبارة "النقود الإلكترونية" **E-money** التي لا تمت بأي صلة بالعملات التشفيرية؟ إنّ هذا الالتباس في المفاهيم والمعاني يؤثّر على نطاق تطبيق القانون بحدّ ذاته، فهل يُطبّق فقط على العملات التشفيرية والرقمية أم أيضاً على النقود الإلكترونية؟

القسم الثاني: جرائم العملات التشفيرية

أصبحت عملة البيتكوين العملة المفضلة لدى المجرم السيبراني[217]، فخصائصها المميزة والتقنيات الحديثة القائمة عليها هي عوامل مغرية ومؤثرة على المجرم وعلى الظاهرة الإجرامية ككل.

بالطبع، ليست العملات التشفيرية بتكوينها وسيلة أو هدف إجرامي، فهي لم تتواجد في الأصل لخدمة المجرمين، وإن ما تتعرض له أو تُستعمل لأجله تتطابق بشكل عام عما تتعرض له النقود الرسمية والورقية والمعدنية. ولكن يكمن الطابع الجدلي بافتقارها إلى تنظيم مستقل وشرعي الأمر الذي أباح وخلق فرصاً إضافية وجذابة أمام شتى أنواع المجرمين. فتواجدها كلياً في نموذج رقمي حال دون مواكبة السلطات المعنية بمرتكبي الأفعال غير المشروعة بواسطتها... وبالرغم من زيادة وتيرة الملاحقات والعمليات الناجحة من إلقاء القبض على هؤلاء، يبقى عدد الأفراد (أو الجهات) الذين نجحوا من الهروب من العدالة أكثر بكثير مقارنةً مع الذين وقعوا بيد السلطات المعنية.

لم تكن البيتكوين والعملات التشفيرية بحد ذاتها مصدر قلق وإرباك إلا بعد ظهور موقع سيلك رود **Silk Road** (طريق الحرير) على شبكة الإنترنت المظلم في العام 2011. بحيث تحوّل مؤسس الموقع روس أولبريخت **Ross Ulbricht** إلى أشهر شخص يدان بارتكابه جرائم تتعلق بالعملات التشفيرية، فهذا الأخير استخدم عملة البيتكوين لبيع المخدرات وتقديم خدمات غير مشروعة على موقعه إلخ. قدّرت الجهات المسؤولة عن إنفاذ القانون المعاملات التي تمت معالجتها عبر الموقع بمبلغ 1.2 مليار دولار بين عامي 2011 و2013. تم إغلاق الموقع في شهر تشرين الأول من العام 2013 من قبل مكتب التحقيقات

217 Steven David Brown. “Cryptocurrency and Criminality: The Bitcoin Opportunity.” The Police Journal, Vol. 89.4, Dec. 2016, pp. 327–339, p. 327.

الفيدرالي **FBI** الذي صادر أرباح "أولبريخت" وكان قد حصد آنذاك ثروة شخصية قدرها 13 مليون دولار على الأقل[218].

من هنا ظهرت علاقة العملات التشفيرية بالجريمة والأفعال غير المشروعة على أنواعها، فبارتفاع قيمتها وازدياد الإقبال عليها شهد العالم إسْتِفحال بوتيرة الجرائم المختلفة الخطورة والتوصيف، فلم يكن أمام الدول خيار غير تدارك خطورة الوضع وضرورة التطرق إلى هذه العملات، وذلك سواء عبر القوانين الداخلية أو بالمعاهدات والأنظمة الدولية العالمية.

من هذا المنطلق، كان من الضروري البحث بالتالي:

الباب الأول: العملات التشفيرية منفذٌ لتمويل الإرهاب

الباب الثاني: الجرائم السيبرانية

---

[218] U.S. Attorney's Office of Southern District of New York, *Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts,* 5 Feb. 2015, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts, Accessed 6 Aug. 2019.

الباب الأول: العملات التشفيرية منفذٌ لتمويل الإرهاب

جميع العمليات الإرهابية بغض النظر عن مدى اتساع نطاقها أو خطورتها، تحتاج إلى التمويل الذي يعادل فعل تمويل الإرهاب من ناحية الأهمية والخطورة. فلولا التمويل ولولا هذه المساندة، لما استطاعت المنظمات الإرهابية من تنفيذ مخططاتها وعملياتها. ولكن اشتداد القيود على التحويلات المصرفية وزيادة الرقابة على الأنظمة والمؤسسات المالية، بدأت تعرقل وتحدّ من حرية عمليات وصفقات تمويل الإرهابيين، فكان البديل السريع لا محال منه.

إن طبيعة العملات التشفيرية وتوفيرها لميزة المجهولية كانت مغرية للمجرمين والإرهابيين، ناهيك عن واقعة عدم صدورها وتنظيمها من قبل السلطات، فكل التحويلات هي خارجة عن الرقابة ومحررة من القيود. فأصبح تمويل الإرهاب وتبييض الأموال السيبراني والإلكتروني في خبر كان وأضحينا أمام منهج تمويل للإرهاب بالعملات التشفيرية. فهل هي البديل الأمثل المنُتظر؟

سنناقش كل ذلك في الفصلين التاليين، الأول بموضوع مفهوم التمويل السيبراني للإرهاب والثاني في التشريع.

الفصل الأول: مفهوم التمويل السيبراني للإرهاب

عندما نتحدث عن إرهاب سيبراني، نتحدث عن إرهاب يُرتكب في الباب الأول عبر شبكة الإنترنت، ومواقع التواصل الاجتماعي والأجهزة الإلكترونية والتكنولوجيا الحديثة، بغض النظر إذا كانت الهدف بحد ذاتها أو مجرد وسيلة.

وطبعاً لم تسلم العملات التشفيرية من أيدي الإرهابيين، فخصائصها ومميزاتها، قدّمت لهم وسيلة جديدة للتمويل والتموُّل بعيداً عن القوانين وسلطات الملاحقة.

وعليه، سنعالج استخدام المنظمات الإرهابية للإنترنت في المبحث الأول، لننتقل إلى موضوع تمويل الإرهاب عبر العملات التشفيرية في المبحث الثاني.

المبحث الأول: استخدام المنظمات الإرهابية للإنترنت

وفّرت الإنترنت ومواقع التواصل الاجتماعي خدمة ومنصة مجانية للمنظمات الإرهابية التي تحاول أن تستغلها بكافة الطرق الممكنة. تمكّنت هذه المنظمات من استغلال عصر المعلومات والبيانات لصالحها، بحيث حقق تدفق المعلومات والبيانات نمواً كبيراً في عملياتها، وذلك طبعاً في غفلة من سلطات الأمن وإنفاذ القانون نظراً لكونهم دائماً على مقدمة منهم، الأمر الذي ساهم بانتشار الظاهرة بسرعة.

اختلفت طرق استغلال الإنترنت والعالم الافتراضي من قبل المنظمات الإرهابية وذلك بهدف زعزعة الأمن الداخلي والدولي. فعلى غرار تسهيل التواصل وتشارك المعلومات، أضحى العالم الافتراضي منبراً لنشر الفكر المتطرّف والدعاية والبروباغندا ومصدراً للتجنيد ووسطاً لجمع الأموال والتخطيط والتنفيذ توصلاً لإحداث الضرر سواء، في العالم المادي أو العالم الافتراضي عبر الهجمات السيبرانية البحت. وهكذا، ظهر الإرهاب السيبراني أو الإلكتروني الذي نقل الإرهاب من العالم المادي إلى العالم الافتراضي.

بالنسبة إلى تعريف الإرهاب السيبراني، فيتقاطع هذا الأخير مع الإرهاب بحيث ليس هنالك من تعريف موّحد، وإن المفهوم والعبارة بحد ذاتها أثارت جدلاً فقهياً واسعاً. فالبعض[219] نكر وجود الإرهاب السيبراني من أصله، معتبرين بأن الاعتداءات والهجمات السيبرانية لا تشكّل خطورة كالإرهاب المادي التقليدي الذي يؤدي إلى الموت والدمار والهلع الأمني والسياسي، فبنظرهم هي ليست إلا هجمات سيبرانية عادية أو حرب معلومات.

أما بالنسبة للبعض الآخر، فالإرهاب الحديث لا يتطلب حصول ضرر مادي ملموس، بل يكفي أن يُحدث الفعل المعيّن حالة الذعر[220]، وإن الإرهاب الإلكتروني قد سبق وأثبت مقدرته على إحداث ضرر مادي في العالم الحقيقي كما في العالم الافتراضي. ولكن، ظهرت الصعوبة عند تصنيف الإرهاب السيبراني[221] والتمييز ما بين الجريمة السيبرانية بشكل عام والهجمات السيبرانية الإرهابية. وبالرغم من كثرة نقاط التشابه، إلا أن الهدف الجرمي والقصد الخاص في الإرهاب السيبراني يبقى مثله مثل الإرهاب، وهو اثارة حالة الذعر أو إلزام السطات من اتخاذ أو عدم اتخاذ موقف معيّن.

تختلف الطرق التي انتهزت بها المنظمات الإرهابية شبكة الإنترنت، فلا بدّ من عرض هذه الطرق بتفصيل أكثر:

---

[219] Eric Chabrow. “Can Cyber Terrorism Exist? – Interview with Jim Harper of the Cato Institute,” Government Info Security News, 10 Jul. 2009, https://www.govinfosecurity.com/interviews/cyber-terrorism-exist-interview-jim-harper-cato-institute-i-283

[220] Michael L. Gross, et al. "The psychological effects of cyber terrorism." Bulletin of the Atomic Scientists, Vol. 72.5, 2016, pp. 284-291.

[221] Victoria Baranetsky. “What is cyberterrorism? Even experts can't agree,” The Harvard Law Record, 5 Nov. 2009, https://web.archive.org/web/20091112093639/http://www.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186

– الدعاية: تعتمد المنظمات الإرهابية بكثرة على شبكة الإنترنت لنشر الدعاية والبروباغندا وإلهام أعمال الإرهاب[222]. فمواقع التواصل الاجتماعي وتطبيقات تواصل أخرى كالتيليغرام **Telegram**، تُستغل للدعاية ونشر الأفكار والخطاب التحريضي والوعود والاغراءات، بهدف استقطاب الشباب وكل من له ميل إلى التطرف. فمجانية المواقع والتطبيقات وعالمية شبكة الإنترنت، أفسحت المجال أمام الارهابي للوصول ببرهة إلى كل زاوية من الكرة الأرضية.

– التجنيد[223]: عززت شبكة الإنترنت الإرهاب الفردي، بحيث يتم استغلال شبكة الإنترنت لإقامة العلاقات مع الذين يتجاوبون مع الدعايات وذلك بهدف التماس الدعم منهم في سبيل مواصلة النشاط الإرهابي. ويتمحور الارتكاز الأكبر على الشباب والقصر، فهؤلاء يمثلون الطبقة الأكبر والأسهل من مستخدمي الإنترنت، فيتم جذبهم عن طريق الرسوم المتحركة وألعاب الحاسوب والفيديوهات التي تغسل عقولهم وتحثّهم على الهجمات الانتحارية وتدفعهم إلى استخدام العنف.

وبدورها، تستخدم مواقع التواصل الاجتماعي للتواصل والايقاع بمن يتوافقون مع الرأي المتطرف، خصوصاً عن طريق الأحاديث الخاصة أو في المجموعات **Social Groups**.

– التدريب الافتراضي: هناك منصات ومواقع إلكترونية وحسابات على مواقع التواصل الاجتماعي، تنشر أدلة عملية وكتيبات ومقاطع فيديوهات ونصائح وشتى التعليمات المطلوبة، وذلك وبلغات عدة بهدف الوصول إلى أكبر عدد ممكن من الجمهور. يتم تفسير طرق الانضمام إلى الجماعة أو المساهمة مادياً أو

---

222 Europol. Report on **Internet Organised Crime Threat Assessment**, Doi 10.2813/858843, 2018, p. 10, www.europol.europa.eu.

223 FATF. Report on **Emerging Terrorist Financing Risks**, Paris, 2015, p. 10, http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

شخصياً عن بعد، على غرار إعطاء التعليمات عن كيفية صنع المتفجرات والأسلحة وكيفية تخطيط وتنفيذ الهجمات.

– التخطيط: المتمثل غالباً بالتواصل والتنسيق عن بعد فيما بين الإرهابيين المتواجدين في مختلف مناطق العالم، فالوظيفة الأساسية للإنترنت هي تيسير الاتصال فيما بين الاشخاص ومنهم الإرهابيين، بحيث يتبادلون المعلومات ويوزعون المهام.

– التنفيذ: تُعتمد شبكة الإنترنت كوسيلة للتأثير على العالم المادي، سواء عن طريق بث التصاريح الخطيرة وإطلاق التهديدات لاستعمال العنف والسلاح بهدف نشر الذعر في المجتمعات، أو عن طريق إحداث الضرر في العالم الافتراضي.

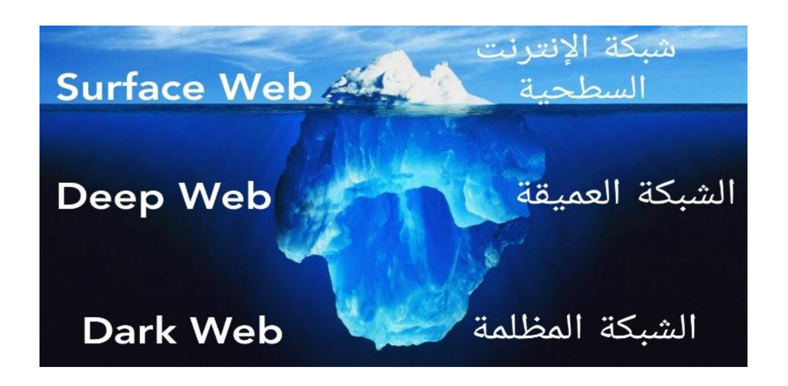
– جيش إلكتروني: تسعى المنظمات الإرهابية جاهدةً إلى لفت الانتباه وإثبات استمرارية وجودها أينما كانت، حتى في العالم الافتراضي. لذلك تعمد إلى استحداث شعب مختصة وتوظف مجاهدين ذي الخبرة في المعلوماتية لينشروا فكر الإرهاب إلكترونياً. وتعمد أيضاً إلى تحريض سائر المتطرفين والمقرصنين على ارتكاب الهجمات الإلكترونية التي تستهدف البنى التحتية الرقمية أو المواقع الإلكترونية خصوصاً تلك الحكومية. إن أثر هذه الهجمات كبيرة وخطيرة، نظراً للتحول الرقمي خصيصاً في القطاع العام والحكومات والإدارات الرقمية، الذي أفسح المجال أمام اختراق قواعد البيانات العامة واستهداف المنظومات الرقمية وما شابه وتعطيل سائر القطاعات، عبر هجمات مثل حجب أو تعطيل الخدمة الموزّعة **DDoS** أو البرامج الخبيثة **Malware**.

وفي مثال حيّ، يسعى التنظيم الإرهابي داعش إلى استقطاب القدرات الشابة من مختلف الجنسيات من أجل أن يساهموا سويا بالتغلغل في العالم الافتراضي والتأثير على الآخرين. فظهر لتنظيم داعش جيشاً إلكترونياً أطلق عليه تسمية "الخليفة السيبرانية..." والتي شنت آلاف الهجمات الإلكترونية متراوحة الخطورة. ولكن، سرعان ما تعاونت سلطات إنفاذ القانون والشركات صاحبة هذه المواقع والخدمات الإلكترونية للحد قدر الإمكان من حرية الإرهابيين من استغلال هذه المنصات الإلكترونية، الأمر الذي دفع بهؤلاء إلى

"النزوح" واعتماد التطبيقات وبرامج التحادث والمنظمات المغلقة القائمة على تقنية التشفير وصولاً إلى عالم الإنترنت المظلم[224] بعيداً عن الشبكة السطحية المرئية.

– **شبكة الإنترنت المظلمة Dark Web:**

تعتبر شبكة الإنترنت المظلم **Dark Net/Dark Web** القسم الباطني الخفي من العالم الافتراضي وهي جزء من شبكة الويب أو الإنترنت العميقة **Deep Web**، والتي بدورها تشكل قسماً من شبكة الويب العالمية أو الشبكة العنكبوتية **World Wide Web**. لا يمكن الولوج إلى الإنترنت المظلم بواسطة محركات البحث مثل **Google** و **Firefox**، بل تستوجب برامج ومحركات بحث خاصة مثل طور **Tor (The Router Onion)** و**I2P (Invisible Internet Project)**[225]. يعتبر محرك أو متصفح **Tor** الأكثر رواجاً، وذلك لأنه أداة لإخفاء هوية المستخدم الرقمية بحيث يتم تشفير حركة المرور الخاصة وإخفاء عنوان البروتوكول **IP Address** الخاصة به. وُجدت في البداية من قبل الحكومة الأميركية كوسيلة للتواصل الخفي وإجراء سائر العمليات بمنأى عن أي تعقب رقمي. في فترة لاحقة تحول الإنترنت المظلم إلى وسيلة بيد الصحافيين والناشطين للتعبير عن رأيهم بحرية، بسبب ميزة إخفاء الهوية وتوفيرها غطاء إضافي من الخصوصية.



4. صورة لجبل جليد يبيّن الفارق بين شبكة الإنترنت السطحية والعميقة

[224] Europol. Report on **Internet Organised Crime Threat Assessment**, Op.cit., p. 52.

[225] Arbër S. Beshiri, and Arsim Susuri. "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review." Journal of Computer and Communications, Vol. 7.3, 2019, pp. 30-43, p. 31.

ولكن سرعان ما تحولت إلى سوقٍ سوداء افتراضية تشمل مواقع تعرض الخدمات والسلع الممنوعة وغير المشروعة والأجهزة التي تسهّل الجرائم السيبرانية والجرائم التقليدية. إن محتوى الإنترنت المظلم يعتبر الأكثر خطورة على الإطلاق في عالم الإنترنت، وذلك لاستضافته مواقع إلكترونية تعرض سلع وخدمات غير مشروعة منها على سبيل المثال لا الحصر: المخدرات، الأسلحة والذخائر، السلع المقلدة والمسروقة، بطاقات الائتمان المسروقة، البيانات المخترقة، جوازات سفر بالإضافة إلى خدمات الكترونية كهجمات حجب أو تعطيل الخدمة الموزّعة **DDoS** والبريد غير المرغوب به **Spam**.

أما وسيلة الدفع المعتمدة من قبل مواقع الإنترنت المظلم؟ فهي تتمثل بالعملات التشفيرية، بحيث تعتبر وسيلة الدفع "الرسمية" والمتعامل بها في السوق السوداء هذه.

وكنتيجة، في ظل كل ميزات الخصوصية والمجهولية الرقمية من جهة، وتوفير وسيلة دفع غير رسمية بعيدة عن رقابة السلطة، تحول الإنترنت المظلم إلى ساحة افتراضية للإجرام وتسهيله.

كان من الطبيعي أن يستغل الإرهابي الإنترنت المظلم، سواء لشراء المواد الممنوعة أو لنشر البروباغندا والأخبار تفادياً لإقفال مواقعهم الإلكترونية الموجودة على الويب السطحي. فنذكر مثلاً موقع سُمي بـ "اصدارات الدولة الاسلامية" والذي تضمن فيديوهات وصور وأخبار تتعلق بالدولة الإسلامية، ولقد اكتُشف الرابط المُحيل إلى الموقع عبر برنامج **Telegram** للمحادثات التشفيرية[226].

[226] Anthony Cuthbertson. "#OpParis: Anonymous pursuit of Isis sees jihadists retreat to the dark web." International Business Times, 18 Nov. 2015, https://www.ibtimes.co.uk/isis-moves-dark-web-escape-anonymous-opparis-1529351, Accessed 22 Apr. 2019.

بالإضافة إلى ذلك، لقد كشفت العديد من سلطات التحقيق بأن بعض الأسلحة المستعملة في عمليات إرهابية كان مصدرها مواقع الإنترنت المظلم، نذكر هجمة ميونيخ في عام 2016[227] وباريس عام 2015[228].

لا مندوحة بأن الإرهاب السيبراني بات يشكل تحدياً جدياً للأمن سواء الداخلي أو الدولي، ولكن هل يمكن مقارنة خطورة الإرهاب السيبراني بالإرهاب المادي؟ فشبكة الإنترنت استحدثت الإرهاب السيبراني وشكلت أداة تسهل العمليات الإرهابية بكافة مراحلها ومنصة لنشر الفكر المتطرف... فهل يأتي اليوم ويُستبدل الإرهاب المادي بذاك السيبراني بشكل مطلق؟ وماذا عن تمويل الإرهاب؟

المبحث الثاني: العملات التشفيرية في عالم تمويل الإرهاب

اختلفت طرق تمويل الإرهاب تاريخياً، فقبل أحداث 11 ايلول من العام 2001، كان الإرهابيون يعتمدون على الطرق والوسائل المشروعة لتلقّي وتحويل الاموال، أبرز هذه الوسائل تمثلت بالعمليات المصرفية واستعمال البطاقات المصرفية. ولكن حادثة 11 أيلول أدّت إلى إحداث ثورة في العالم التشريعي سواء على صعيد المجتمع الدولي أو الداخلي لناحية القوانين والإجراءات التي ترعى تبييض الأموال وتمويل الإرهاب، الأمر الذي ضيّق على المنظمات الإرهابية وعثّر استعمالهم الوسائل المشروعة المعتمدة عالمياً لنقل وتحويل الأموال.

227 Ruth Bender, and Christopher Alessi. "Munich Shooter Likely Bought Reactivated Pistol on Dark Net." The Wall Street Journal, 24 Jul. 2016, https://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686, Accessed 19 Apr. 2019.

228 Nikita Malik. "How The Darknet Can Be Used By Terrorists To Obtain Weapons." Forbes, 15 Jan. 2019, https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/, Accessed 21 Apr. 2019.

وكنتيجة، ونظراً لشدة الرقابة المفروضة جراء قوانين ومعاهدات مكافحة تبييض الأموال وتمويل الإرهاب وخصوصاً قيام التعاون الوثيق بين القطاعين العام والخاص وقواعد "اعرف عميلك" "**Know Your Customer**"، اضطرت المنظمات الإرهابية إلى البحث عن وسائل وطرق جديدة تمكنها من الحصول على التمويل بعيداً عن أنظار سلطات إنفاذ القانون. اختلفت هذه الوسائل من شرعية كالتجارة بالبترول والغاز إلى غير شرعية ناتجة عن ارتكاب أفعال جرمية. وطبعاً، كثر اعتماد نظام الحوالة المالية، الذي يعتبر وسيلة غير مشروعة تمكّن من تحويل الأموال إلى أي مكان عن طريق شبكة غير رسمية تقع خارج نطاق الأنظمة المصرفية، بحيث يغلب عنصر الثقة بشكل رئيسي على التعامل بين أطراف العملية أي الوسيط المرسل والوسيط المستلم، وذلك جراء تسوية متفق عليها من قبل الطرفين. على غرار نظام الحوالة المالية، لجأ الإرهابيون إلى الأفعال الجرمية كمصدر لجمع الأموال[229]. فمثلاً، أفادت تقارير بأن تنظيم القاعدة في بلاد المغرب الإسلامي نجح بتحصيل 100 مليون دولار أميركي جراء عمليات خطف وابتزاز مقابل فدية مالية، بالإضافة إلى أرباح الناتجة عن الاتجار بالمخدرات والأشخاص[230].

ولكن مع التطور الرقمي، كان من المتوقع استغلال الإرهابيين للتكنولوجيا لتحقيق مصالحهم، بحيث نجح هؤلاء في إيجاد وسيلة جديدة وعصرية للتمويل بعيداً عن أنظار سلطات إنفاذ القانون، وذلك عن طريق العملات التشفيرية. فهذه العملات تتسم بتقنيات حديثة تمكّن المنظمات الإرهابية من الحصول على الأموال بدون قيود ولا رقابة، بحيث يفلتون بكل سهولة من الانكشاف، خصوصاً بسبب استفادتهم من غطاء المجهولية التي توفرها... هذا على غرار مميزات أخرى كإمكانية التحويل الفوري من وإلى أي عملة نقدية

229 Iwa Salami. “Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?”, Studies in Conflict & Terrorism, Vol. 41.12, 2018, pp. 968-989, p. 971.

230 Yaya Fanusie, and Alex Enetz. Report on **Al-Qaeda in the Islamic Maghreb Financial Assessment**, Center on Sanctions & Illicit Finance, 2017, p. 3.
https://www.fdd.org/analysis/2017/12/07/terror-finance-briefing-book/

رسمية، السرعة في العمليات المالية، الطابع الدولي، رسوم التحويلات الزهيدة، والأهم إمكانية استعمال هذه العملات على شبكة الإنترنت المظلم.

رحّبت المنظمات الإرهابية بهذه العملات وراحت تنشر طرق التعامل بها وإرسالها عبر مواقع التواصل الاجتماعي والشبكة العالمية بشكل عام. تاريخياً، بدأ رواج العملات التشفيرية كوسيلة لتمويل الإرهاب في العام 2014. وفي قضية فريدة من نوعها، حاكمت محكمة في ولاية فيرجينيا الأميركية في العام 2015 مؤيد للدولة الاسلامية بعد أن نشر مقالاً بعنوان "البيتكوين وصدقة الجهاد" على موقع التواصل الاجتماعي "تويتر"، بحيث شجّع على استعمال البيتكوين كوسيلة بديلة للنظام المالي العالمي، واغتنام ميزة "عدم إمكانية التعقب" **Untraceability** كبديل لجمع الأموال[231].

إن امتلاك الإرهابيين حسابات على مواقع التواصل الاجتماعي ليس بالأمر الجديد، فهؤلاء يستغلون هذه الحسابات أيضاً لطلب التمويل بسائر الطرق وحتى بالعملات التشفيرية. ولقد برزت عدة حسابات تابعة لمنظمات إرهابية على موقع تويتر، منها باسم "الصدقة" "**Al Sadaqah** " والتي دعمت الثوار في دولة سوريا وقبلت التبرعات بالعملات التشفيرية لحين إغلاقها، ولقد تم لاحقاً ربط هذا الحساب بتنظيم القاعدة[232]. ومن مواقع التواصل الاجتماعي الموجودة على شبكة الويب السطحية، انتقل الإرهابيون إلى شبكة الإنترنت الباطنية المظلمة، بحيث تم اكتشاف العديد من الرسائل على مواقع كائنة في الشبكة المظلمة منشورة من

---

231 U.S. District Court Judge in Eastern District of Virginia, *Virginia Teen Pleads Guilty to Providing Material Support to ISIL*, Press release No. 15-727, 11 Jun. 2015, https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil

232 Tom Keatinge, et al. Study commissioned by European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, on "**Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses: Counter-terrorism**," No. PE 604.970, May 2018, p. 34.

قبل مناصري[233] هذه المنظمات تدعو إلى تمويل الدولة الإسلامية وغيرها عبر عملة البيتكوين التشفيرية، وذلك طبعاً بعد نشر وتعميم عنوان محفظة معيّنة تابعة للمنظمة[234].

وبالطبع، اختلفت طرق تمويل الإرهابيين عن طريق العملات التشفيرية، وتنوّعت الملاحقات القضائية، فمؤخراً اعترفت امرأة في ولاية نيويورك الأميركية بتمويل تنظيم الدولة الإسلامية عن طريق عملة البيتكوين. وفي الحيثيات، تم الكشف بأن السيدة بعدما نجحت بالحصول على مبالغ مالية ناتجة عن أعمال احتيالية مصرفية، أقدمت على تبييض ألاف الدولارات وإرسالها إلى تنظيم الدولة الإسلامية[235].

ولكن واقعة مدى اعتماد هذه العملات كوسيلة ومصدر رئيسي لتمويل الإرهاب، أدى إلى نشوء جدل فقهي فيما بين الأكاديميين. فالبعض[236] يشدد على خطورة الوضع خصوصاً بعدما عمد مؤيدي تنظيم الدولة الإسلامية على نشر أدلة إرشادية عدة تفسّر إلى الجمهور عملية إرسال الأموال عن طريق العملات

---

[233] من هؤلاء نذكر المناصر المعروف بأبو أحمد الرقة الذي كان ينشر عناوين بيتكون تابعة لـ Official Islamic State Funding Center.

[234] Adam Taylor. "The Islamic State (or someone pretending to be it) Is Trying To Raise Funds Using Bitcoin." The Washington Post, 9 Jun. 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin/?noredirect=on&utm_term=.c7404e464ffb, Accessed 19 Apr. 2019.

[235] Federal Court in Central Islip New York, *Long Island Woman Pleads Guilty to Providing Material Support to ISIS*, Docket No. 17-CR-690 (JS), 26 Nov. 2018. https://www.justice.gov/usao-edny/pr/long-island-woman-pleads-guilty-providing-material-support-isis

[236] Celina Realuyo. "North American Effort to Combat the Financing of Terrorism." **SOF Role in Combating Transnational Organized Crime**, The JSOU Press MacDill Air Force Base, Florida, 2016, pp. 85-108, p. 101.

التشفيرية. الأمر الذي استتبع ولجدية الوضع إطلاق الانذار من قبل مجموعة العمل المالي **FATF** لجهة استغلال العملات التشفيرية لتمويل الإرهابيين وتخبئة محاصيلهم الجرمية[237].

في المقابل، يرى البعض الآخر[238] بأن واقعة استعمال الإرهابيين للعملات التشفيرية ليست بتلك الجدية ولا تدعو إلى التأهب، معتبرين أن هذه العملات وخصوصاً البيتكوين ليست بالوسيلة الفضلى والمعتمدة بشكل رئيسي من الإرهابيين.

كما أقر البعض[239] بأن عملة البيتكوين ليست بالمصدر الجدي والموثوق به من قبل الجهاديين في الوقت الراهن، ولكن لا شيء يضمن عدم انقلاب الوضع في المستقبل، مؤكدين بأنه ليس هنالك ما يمنع من ظهور عملة تشفيرية أو رقمية جديدة تتصف بمميزات خصوصية ومجهولية أكثر، توفر مهرباً أكيداً من قوانين وأنظمة مكافحة تبييض الأموال وتمويل الإرهاب.

لا مندوحة بأن المنظمات الإرهابية وجدت في البيتكوين والعملات التشفيرية بشكل عام، مهرباً لا بأس به من القيود المفروضة على الوسائل التقليدية والمشروعة لتحويل الأموال وتلقيها. برأينا، إن العملات التشفيرية هي أداة بيد المنظمات الإرهابية تمكّنهم من تحصيل الأموال وتمويل عملياتهم، على غرار منحهم وسيلة حرة من الرقابة نوعاً ما أثناء تحويل الأموال عالمياً... ولكن تكمن الإشكالية في مدى قدرة المنظمات الإرهابية بالاستناد كلياً على العملات التشفيرية كبديل للنقود التقليدية، بالتأكيد هذا ليس بالأمر المستحيل،

---

237 FATF. “Regulation of Virtual Assets,” Paris, October 2018, Accessed 22 Oct. 2018, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/regulation-virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

238 David Manheim, et al., “Are Terrorists Using Cryptocurrencies?” Foreign Affairs, 21 Apr. 2017, https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies

239 Yaya Fanusie. “Terrorist Networks Eye Bitcoin as Cryptocurrency’s Price Rises,” The Cipher Brief (blog), 21 Dec. 2017, https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises

ولكن في الوقت الراهن تبقى هذه العملات مجرد وسيلة وأداة ثانوية وتكميلية ينتفع منها هؤلاء. فالبنى التحتية المطلوبة لاعتماد العملات التشفيرية تشكّل تحدّياً كبيراً، فمعظم المنظمات الإرهابية متمركزة في مناطق فقيرة من الساحل الأفريقي واليمن والعراق وسوريا والتي تفتقر للبنى التحتية لا سيما التقنية منها. فهذا عائق كبير لجهة تبني العملات التشفيرية بصورة اساسية، فبدون البنى التحتية المتطورة لن يتمكن هؤلاء من اعتماد العملات التشفيرية على نطاق واسع. من جهة ثانية، إن التعامل مع العملات التشفيرية حالياً في هذه المناطق هي معدومة، الأمر الذي يعوق اعتماد واستثمار الإرهابيين للعملات التشفيرية كنقود لقاء شراء حاجياتهم سواء المعيشية أو العملية.

حالياً، ينجح الإرهابي من التحايل على الأنظمة العالمية المالية والقانونية لتسيير أموره المالية، وتبقى العملات التشفيرية في مراحلها الأولية كوسيلة ثانوية موثوقة لتمويل الإرهاب. ولكن هل من الممكن أن نشهد في المستقبل هجمات ارهابية ممولة كلياً بالعملات التشفيرية؟ وما موقف المشرع الداخلي والدولي حيال ذلك؟

الفصل الثاني: في التشريع

تمثّلت أول المبادرات لتشريع وتنظيم العملات التشفيرية عبر إدخالها في القوانين والأنظمة المختصة بمكافحة تبييض الأموال وتمويل الإرهاب.

فيغدو لتاريخنا هذا النهج هو الأكثر اتباعاً والأكثر اعتماداً سواء في النطاق الدولي والإقليمي أو الداخلي. ففي حين عدّل البعض أنظمة كانت أصلاً قائمة، اختار البعض الآخر سنّ نصوص حديثة متخصصة. وبالتالي، سنبحث في المبحث الأول الموقف الدولي والإقليمي، لنعالج بعض المواقف الداخلية في المبحث الثاني.

المبحث الأول: الموقف الدولي والإقليمي

سنعمد إلى تعداد أهم وأبرز الواقف المتخذة دولياً وإقليمياً حيال العملات التشفيرية في مجال تمويل الإرهاب.

أولاً. الأمم المتحدة:

وضع المجتمع الدولي منذ عام 1963، 13 صكاً قانونياً لمكافحة الأعمال الإرهابية. لقد أُعدَّت هذه الصكوك بإشراف الأمم المتحدة والوكالة الدولية للطاقة الذرية وسائر وكالاتها المتخصصة، على غرار قرارات صادرة عن مجلس الأمن. وفيما بعد، أدخل المجتمع الدولي بعضاً من التغييرات الجوهرية على ثلاثة من هذه الصكوك العالمية واعتمدت بضعة تعديلات ووافقت على بروتوكولات وصكوك أخرى تهدف إلى قمع ومكافحة الإرهاب من كافة النواحي[240].

---

[240] مكتب مكافحة الإرهاب–الأمم المتحدة فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب، " الصكوك الدولية لمكافحة الإرهاب"، الأمم المتحدة، https://www.un.org/counterterrorism/ctitf/ar/international-legal-instruments

ولما كان الإرهاب بحاجة إلى التمويل فبدونه تبقى المخططات حبراً على ورق... سرعان ما استدرك المجتمع الدولي ضرورة بذل جهود متساوية لجهة مكافحة وقمع تمويل الإرهاب، فوضعت الأمم المتحدة في العام 1999 الاتفاقية الدولية لقمع تمويل الإرهاب **Terrorist Financing Convention** [241]، تهدف إلى تجريم أفعال تمويل الإرهاب[242] وتسعى إلى تعزيز التعاون بين سلطات إنفاذ القانون والقضاء بغية قمع، واجراء التحقيقات اللازمة توصلاً لمعاقبة مرتكبي مثل هذه الأفعال.

مباشرةً بعد هجمات 11 أيلول من العام 2001 الإرهابية التي استهدفت الولايات المتحدة، تبنى مجلس الأمن بالإجماع القرار رقم 1373 [243] والذي دعا إلى تجريم ومنع تمويل الأعمال الإرهابية، وتجميد كافة مصادر التمويل، ومشاركة المعلومات فيما يتعلق بالجماعات الإرهابية. أما الدول التي ترفض التعاون في حملات مكافحة الإرهاب وتمويله، فهي عُرضة للعقوبات وفقاً للفصل السابع من ميثاق الأمم المتحدة. وبموجب القرار نفسه وكآلية لحسن تنفيذه، أنشأ مجلس الأمن لجنة مكافحة الإرهاب **Counter Terrorism Committee**، وكلفها بالقيام بدور رقابي على دول الأعضاء ومتابعة مدى استجابة هؤلاء لمتطلبات القرار 1373.

انشأت الأمم المتحدة على مدار السنين العديد من اللجان والمكاتب والهيئات التي تُعنى بمواضيع الإرهاب وتمويله، ولعل من أبرز ما استحدثث هو مكتب الأمم المتحدة لمكافحة الإرهاب **United**

---

[241] الاتفاقية الدولية لقمع تمويل الإرهاب قرار رقم 109/54 لسنة 1999، www.treaties.un.org

[242] تعرّف المادة 2.1 من الاتفاقية الدولية لقمع تمويل الإرهاب جريمة تمويل الإرهاب على النحو التالي:
" يرتكب جريمة بمفهوم هذه الاتفاقي، كل شخص يقوم بأية وسيلة كانت، مباشرة أو غير مباشرة، وبشكل غير مشروع وبإرادته، بتقديم أو جمع أموال بنية استخدامها، أو هو يعلم أنها ستستخدم كلياً أو جزئياً، للقيام:
أ) بعمل يشكل جريمة في نطاق إحدى المعاهدات الواردة في المرفق وبالتعريف المحدد في هذه المعاهدات؛
ب) بأي عمل آخر يهدف إلى التسبب في موت شخص مدني أو أي شخص آخر، أو إصابته بجروح بدنية جسيمة، عندما يكون هذا الشخص غير مشترك في أعمال عدائية في حالة نشوب نزاع مسلّح، عندما يكون غرض هذا العمل، بحكم طبيعته أو في سياقه، موجهاً لترويع السكان، أو لإرغام حكومة أو منظمة دولية على القيام بأي عمل أو الامتناع عن القيام به."

[243] قرار مجلس الأمن رقم 1373 تاريخ 28 أيلول 2001، /www.un.org/en/ga

(UNOCT) Nations Office of Counter-Terrorism[244] في العام 2017. يضطلع المكتب بالعديد من المهام أهمها منع ومكافحة الإرهاب، وتعزيز تقديم المساعدة في بناء قدرات الدول الأعضاء على تقفي الإرهاب ومكافحته في بيئة كائنة على التنسيق والاتساق بين دول الأعضاء والأمم المتحدة.

- **<u>قرار مجلس الأمن رقم 2019/2462</u>**[245]

على الرغم من تناول موضوع تمويل الإرهاب بموجب معاهدات وقرارات منذ سنوات، تبنى مجلس الأمن في آذار من العام 2019 بموجب الفصل السابع من شرعة الأمم المتحدة وبالإجماع القرار رقم 2462.

يلزم القرار بموجب الفقرة الخامسة من مقدمته، جميع الدول الأعضاء من التأكد بأن قوانينها وأنظمتها المحلية تجرّم تمويل الإرهاب بوصفها من الجرائم الخطيرة، ويدعو في الفقرة الثامنة على تطبيق عقوبات ذات الوصف الجنائي تكون متناسبة ورادعة. ويطالب القرار أيضاً الدول الأعضاء بتجريم تمويل الإرهاب بما يتماشى مع التوصية رقم 5 لمجموعة العمل المالي **FATF**؛ مع التدارك بأنه يتعين على الدول تجريم تمويل العمل الإرهابي وأيضاً تمويل دعم الجماعات الإرهابية والإرهابيين الأفراد وذلك لأي غرض كان، أي حتى في حالة انعدام الصلة بعمل إرهابي محدد. هذا أمر بالغ في الأهمية، فتمويل عمل إرهابي واحد قد لا يتطلب مبلغًا مالياً كبيرًا، ولكن الحفاظ على منظمة إرهابية بأكملها وتطويرها يتطلب موارد مالية كبيرة.

ما يميّز هذا القرار بأنه أول قرار شامل ومتكامل حول تمويل الإرهاب يصدر عن الأمم المتحدة، والذي يتطرق إلى العملات التشفيرية وذلك تحت عبارة "الأصول الافتراضية" **Virtual assets**. أعرب

---

[244] قرار الجمعية العامة رقم A/RES/71/291، الجلسة 71، 19 حزيران 2017، /www.un.org/en/ga

[245] قرار مجلس الأمن رقم 2462 تاريخ 28 آذار 2019،

https://www.un.org/securitycouncil/content/sres24622019

القرار القلق البالغ من استغلال الإرهابيين والجماعات الإرهابية طرق الدفع الحديثة مثل البطاقات المسبقة الدفع أو الدفع بواسطة الهواتف الذكية أو "الأصول المالية الافتراضية"[246].

ورحّب القرار في الفقرة رقم (21)[247] منه عمل مجموعة العمل المالي المستمر لجهة الأصول الافتراضية وما سمّته بـ "مقدمي خدمات الأصول الافتراضية" **Virtual Assets Service Providers**، بما في ذلك التعديلات التي أدخلتها في شهر تشرين الأول من العام 2018 إلى معاييرها والبيان المتعلق بـ "التنظيم القانوني للأصول الافتراضية" **Regulation of Virtual Assets**. كما أنه شجع الدول الأعضاء على تطبيق اللوائح التنظيمية الخاصة وسن قوانين وأنظمة مكافحة تبييض الأموال وتمويل الإرهاب على مقدمي خدمات الأصول الافتراضية، وعلى ترسيخ نظم فعالة لإجراء الرصد أو الإشراف القائمين على أساس المخاطر على مقدمي هذه الخدمات.

يحثّ القرار دول الأعضاء إلى التحرك لتحسين آلية التعقّب وتعزيز الشفافية لناحية كشف سرية التحويلات المالية، وتطوير وسائل لمراقبة حركة المدفوعات عبر الهواتف الذكية واستخدام الأصول والعملات الافتراضية والتشفيرية.

---

[246] Preamble of the Security Council resolution n.2462/2019:

"Further noting with grave concern that terrorists, including foreign terrorist fighters, and terrorist groups may move and transfer funds, including through financial institutions, abuse of legitimate businesses and non-profit organizations, including as front businesses and organizations and cash-couriers, as well as through the use of emerging payment methods, such as prepaid cards and mobile-payments or virtual-assets."

[247] Par. n. (21), ibid.تصحيح

"Welcomes in that regard FATF' s ongoing work concerning virtual assets and virtual assets service providers, including its October 2018 amendments to the FATF standards and statement on the Regulation of Virtual Assets, and encourages Member States to apply risk-based anti-money laundering and counter-terrorist financing regulations to virtual asset service providers, and to identify effective systems to conduct risk-based monitoring or supervision of virtual asset service providers;"

من الملاحظ بأن الأمم المتحدة ستتبنى الأنظمة والقواعد التي ستقوم مجموعة العمل المالي بوضعها فيما يتعلق بالعملات التشفيرية أو "الأصول الافتراضية" وبمقدمي خدمات هذه الأصول، وذلك في إطار قمع وكشف ومكافحة تمويل الإرهاب بواسطتها، ولقد أقرّت بالدور الأساسي لمجموعة العمل المالي في وضع معايير عالمية لمكافحة تبييض الأموال وتمويل الإرهاب. إن هذه الخطوة إيجابية وتدل على استدراك الأمم المتحدة مدى امكانية استغلال العملات التشفيرية في مثل هذه الأفعال الخطيرة، وتبيّن نيّتها في متابعة الموضوع عن كثب في المستقبل القريب. فهل نرى قريباً معاهدة خاصة تتناول العملات التشفيرية كوسيلة لتمويل الإرهاب مذيّلة بتوقيع الأمم المتحدة؟

ثانياً. الموقف الإقليمي:

– **التوجيه الأوروبي الخامس لمكافحة تبييض الأموال رقم 2018/843**[248]:

ناقشنا في إطار بحثنا بأن التوجيه الأوروبي الخامس لمكافحة تبييض الأموال **AMLD5** يعتبر الصك القانوني الرئيسي في أوروبا الذي يضع الأسس القانونية لمنع استغلال الأنظمة المالية لتبييض الأموال وتمويل الإرهاب، وأنه أدخل تعديلات تتعلق بالعملات التشفيرية والعملات الافتراضية[249] هي الأولى من نوعها على الصعيد الإقليمي الأوروبي.

وكما رأينا مسبقاً، بأن التوجيه لحظ أهمية وضرورة إخضاع مقدمي خدمات المحفظة **CWP** ومنصات العملات الافتراضية **VCE** لموجب كشف الحركات المشبوهة، نظراً لإمكانية استغلال الجماعات الإرهابية لهذه الخدمات لنقل الأموال عبر الأنظمة المالية أو شبكات العملات الافتراضية، عن طريق إخفاء

[248] Council of Europe: Directive 843/2018 of the European Parliament and of the Council of 30 May 2018 amending Directive 849/2018 on the prevention of the use of financial system for the purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, **Official Journal of the European Union**, L.156, 19 Jun. 2018.

[249] استُعمل في متن التوجيه مصطلح Virtual Currencies أي العملات الافتراضية.

التحويلات أو الاستفادة من درجات معينة من المجهولية[250]. وعملاً بالتعديلات الجديدة، وللتخفيف من وطأة ميزة المجهولية، أضحت الجهات المعنية ملزمة على جمع معلومات عن عملائها على غرار بعض الجهات الثالثة التي ليست بعلاقة مباشرة مع هذه الجهات (كالمالك المستفيد). لا بل أصبح بإمكان السلطات المحلية الحصول من مقدمي الخدمات المذكورة على البيانات والمعلومات كافة، التي تمكّنهم من ربط عناوين العملات الافتراضية بهوية أصحابها[251]. هكذا، ستتمكن السلطات المختصة من مطابقة جميع الحسابات المصرفية وحسابات الدفع مع مالكي الحسابات وأصحاب المالكين المستفيدين، مما يعني القضاء على خاصية المجهولية في النطاق المحدد.

وبالإضافة إلى ذلك، لقد اشترطت المادة 44 (فقرة 29) من التوجيه التسجيل المسبق من قبل مقدمي خدمات المحفظة **CWP** ومنصات العملات الافتراضية لدى السلطات المحلية لتتمكن من ممارسة نشاطها. فسيتعيّن على هؤلاء أخذ إجراءات تختص بالتدقيق الإلزامي لمعطيات العملاء **Customer Due Diligence** ومراقبة المعاملات والإبلاغ عن أي نشاط مشبوه إلى السلطات الوطنية المختصة.

ماذا تعني كل هذه التعديلات؟

لا مندوحة بأن التوجيه الخامس يسعى إلى توفير الشفافية في عالم العملات التشفيرية، وإن هذه التعديلات تعتبر بداية جيدة نحو إحاطة هذه العملات بالغطاء التشريعي، إلا أن هناك بعضاً من الثغرات التي تستوجب البحث. كما ذكرنا مسبقاً، إن التوجيه يسلب المجهولية عن المستخدمين الذين يتعاملون حصراً بواسطة مقدمي خدمات المحفظة ومنصات العملات الافتراضية، إلا أنه هناك سبل أخرى لتخزين والتعامل بالعملات التشفيرية والتي تقع حكماً خارج نطاق أحكام التوجيه، مما يعني عدم زوال غطاء المجهولية عن الكافة وعدم إحاطة كافة سبل التعامل.

[250] AMLD 5 recital (8).

[251] AMLD 5 recital (9).

ولناحية منصات تحويل واستبدال العملات التشفيرية، فالتوجيه يشمل منصات التحويل فيما بين النقود الرسمية والعملات التشفيرية، دون تلك التي تُعنى فقط بالتبادل فيما بين العملات التشفيرية (**Crypto to Crypto**)، وتعتبر هذه الواقعة فجوة كبيرة في التوجيه. أما واقعة منح حق التسجيل أو التصريح الاختياري للجهات والأشخاص الذين يقعون خارج نطاق أحكام التوجيه، فهو بتدبير ليس بالفعّال، فالذي يجري عمليات غير قانونية أو مشبوهة لن يصرّح طوعاً عن عملياته وعملاته التشفيرية... فيبقى التسجيل الإلزامي هو الحل الأنسب[252] إذا ما كانت هناك نية جدية.

ومن المنظار الدولي، ننتقل إلى المواقف الداخلية لنعرض بعضاً من السبل التي عالجت بها الدول العملات التشفيرية في نطاق تمويل الإرهاب.

المبحث الثاني: الموقف الداخلي

سنعمد في هذا الشق البحث في أهم وأبرز المواقف التشريعية المتخذة في النطاق الداخلي.

أولاً. التشريع الإستوني:

في نهاية عام 2017، انضمت إستونيا إلى فئة الدول الأوروبية الأولى التي سنتّ التشريعات والقوانين الراعية لتداول العملات التشفيرية. فاشترطت نوعين من التراخيص[253]، الأولى على من يرغب بتشغيل منصة معاملات وتحويل فيما بين النقود الرسمية والعملات التشفيرية. والترخيص الثاني يسمح بتقديم خدمات محفظة العملات التشفيرية. ذلك طبعاً مع الامتثال بشرط رئيسي متمثل بضرورة تسجيل الشركة المعنية في إستونيا.

---

[252] Robby Houben, and Alexander Snyers. Study requested by the European Parliament's TAX3 Committee, on "**Cryptocurrencies and Blockchain Legal Context and Implications for Financial-Crime, Money Laundering and Tax Evasion**," No. PE 619.024, Brussels, July 2018, p. 80, http://www.europarl.europa.eu/committees/en/supporting-analyses-search.html

[253] Chapter 8 (section70) of the Estonian "Money Laundering and Terrorist Financing Prevention Act" of November 27, 2017.

تصدر التراخيص من وحدة الاستخبارات المالية الإستونية **Financial Intelligence Unit** (مختصر **FIU**)، وهي وحدة هيكلية مستقلة تابعة لمجلس الشرطة وحرس الحدود الإستونية **Estonian Police and Border Guard Board**. تخضع طلبات الترخيص إلى إجراءات مكافحة تبييض الأموال وتمويل الإرهاب المحلية[254] والدولية[255] خصوصاً قاعدة "اعرف عميلك".

إلا أن الحكومة الإستونية تعمل مؤخراً وبوتيرة مكثفة على تشديد القوانين المتعلقة بمنح التراخيص للشركات التي تعمل في مجال العملات التشفيرية. ستشمل التغييرات كلاً من متطلبات وشروط الترخيص وعملية تقديم الطلب، وذلك امتثالاً مع التوجيه الأوروبي الخامس **AMLD5** الذي يشدد من إجراءات مكافحة تمويل الإرهاب وتبييض الأموال. وبالتالي، ستعمد وحدة الاستخبارات المالية الاستونية **FIU** إلى اجراء التحقيق الدقيق حول طالبي التسجيل قبل منح أي الترخيص.

ثانياً. التشريع الكندي:

أشرنا مسبقاً في دراستنا إلى أن كندا كانت أول دولة تعالج العملات الرقمية في قوانينها[256] وذلك عبر اخضاعها لأحكام قانون مكافحة تبييض الأموال وتمويل الإرهاب الكندي[257]. وضع هذا القانون منصات العملات الرقمية بخانة الأعمال المختصة بالخدمات المالية **MSB** (**Money Service**

[254] "Money Laundering and Terrorist Financing Prevention Act", Loc.cit.

[255] كانت إستونيا أول دولة تطبق التوجيه الأوروبي الخامس قبل دخوله حيّز التنفيذ، بحيث اعتمدت على نص مسودة التوجيه لتعديل قوانينها المحلية.

[256] Christine Duhaime. "Canada Implements World's First National Bitcoin Law," DUHAIME LAW, 22 Jun. 2014, https://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/, Accessed 19 Sept. 2019.

[257] Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019: SOR/2019-240, Canada Gazette, Part II, Volume 153, Number 14, 10 July 2019.

Businesses)، مما يعني الزامية خضوعها إلى الترخيص المسبق من قبل وكالة FINTRAC [258]، وتطبيق كافة الأحكام والقواعد التي ترعى مكافحة تبييض الأموال وتمويل الإرهاب[259].

ثالثاً. التشريع اللبناني:

جُرّم فعل تمويل الإرهاب بنصٍّ مستقل لأول مرة في لبنان بموجب القانون رقم 533 [260] تاريخ 20 تشرين الأول 2003 عبر المادة 316 مكرر، معدلاً بذلك قانون العقوبات اللبناني. وتبنى المشرع اللبناني في العام 2015 منظومة تشريعية في مجال مكافحة تبييض الأموال وتمويل الإرهاب وذلك بهدف مواكبة المعايير الدولية، وانصياعاً للتوصيات الصادرة عن مجموعة العمل المالي FATF ومنظمة العمل الاقتصادي والتنمية OECD وتطبيقاً للاتفاقيات المتعلقة بمكافحة تمويل الإرهاب، وكمبادرة جدية لبيان جهوده في مكافحة تمويل الإرهاب. فأقر المجلس النيابي باقة من مشاريع القوانين أهمها:

قانون تبييض الأموال وتمويل الإرهاب رقم 2015/44 [261] الذي يجرم تمويل أنشطة الإرهابيين بحسب ما ذُكر في قرار مجلس الأمن رقم 2178، كما وضع الأسس القانونية التي أتاحت بدورها وضع آليات خاصة لتطبيق العقوبات المالية بهدف تنفيذ قرار مجلس الأمن رقم 1267، والقانون المتعلق بالتصريح

---

[258] Financial Transactions and Reports Analysis Centre of Canada

[259] Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019: SOR/2019-240, Loc.cit.

[260] قانون رقم 553 تاريخ 2003/10/20، الجريدة الرسمية، عدد 48 تاريخ 2003/10/22، ص. 188(إضافة مادة جديدة إلى قانون العقوبات).

المادة 316 مكرر (القديمة):

"كل من يقوم عن قصد وبأية وسيلة مباشرة أو غير مباشرة بتمويل أو المساهمة بتمويل الإرهاب أو الأعمال الإرهابية أو الجماعات الإرهابية يعاقب بالأشغال الشاقة المؤقتة لمدة لا تقل عن ثلاث سنوات ولا تزيد عن سبع سنوات وبغرامة لا تقل عن مثل المبلغ المدفوع ولا تزيد عن ثلاثة أمثاله."

[261] قانون رقم 44 تاريخ 2015/11/24، الجريدة الرسمية، عدد 48 تاريخ 2015/11/26، الصفحات 3313-3318 (قانون مكافحة تبييض الأموال وتمويل الإرهاب).

عن نقل الأموال عبر الحدود[262] رقم 42 تاريخ 24 تشرين الثاني 2015، والقانون المتعلق بالإجازة للحكومة اللبنانية بالانضمام إلى الاتفاقية الدولية لقمع تمويل الإرهاب[263] الموقعة في نيويورك سنة 1999 وذلك بموجب القانون رقم 53 [264] تاريخ 24 تشرين الثاني 2015[265].

من جهته، يلعب المصرف المركزي دوراً أكثر من بارز في مجال مكافحة تمويل الإرهاب خصوصاً على الصعيد العملي والتنفيذي، بحيث يواصل بذل الجهود واتخاذ الإجراءات المطلوبة وإصدار الأنظمة اللازمة لمكافحة وتمويل الإرهاب وتبييض الأموال عبر القرارات والتعاميم، أبرزها القرار الأساسي رقم 7818 تاريخ 18 أيار 2001 مع تعديلاته والمتعلق بنظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال وتمويل الإرهاب والقرار الأساسي رقم 12836 تاريخ 26 حزيران 2018 المتعلق بمكافحة تبييض الأموال وتمويل الإرهاب[266] [267].

---

[262] قانون رقم 42 تاريخ 2015/11/24، الجريدة الرسمية، عدد 48 تاريخ 2015/11/26، الصفحات 3310-3312 (التصريح عن الأموال عبر الحدود).

[263] "International Convention for the Suppression of the Financing of Terrorism", General Assembly, n. A/RES/54/109, 54th session, 9 Dec. 1999.

[264] قانون رقم 53 تاريخ 2015/11/24، الجريدة الرسمية، عدد 48 تاريخ 2015/11/26، (الإجازة للحكومة اللبنانية الانضمام إلى الاتفاقية الدولية لقمع تمويل الإرهاب الموقعة في نيويورك بتاريخ 1999/12/9).

[265] بالإضافة إلى دخول كل من آلية تنفيذ قرار مجلس الأمن رقم 1999/1267 والقرارات اللاحقة له، وآلية تطبيق قرار مجلس الأمن رقم 2001/1373 والقرارات اللاحقة له حيّز التنفيذ وذلك في العام نفسه أي سنة 2015.

[266] بالإضافة إلى القرار الأساسي رقم 12147 تاريخ 2015/12/22، الجريدة الرسمية، عدد 53 تاريخ 2015/12/31، الصفحات 3880-3879 (المتعلق بتطبيق قرارات مجلس الأمن رقم 1999/1267 ورقم 2011/1989 ورقم 2011/1988 والقرارات اللاحقة).

[267] مصرف لبنان، قرار أساسي رقم 12836 تاريخ 2018/6/26، الجريدة الرسمية، عدد 30 تاريخ 2018/7/5 الصفحات 3981-3982 (المتعلق بمكافحة تبييض الأموال وتمويل الإرهاب).

ولعله يعتبر مصرف لبنان أول من تطرق في لبنان إلى العملات التشفيرية، بموجب الإعلام رقم 900 تاريخ 19 كانون الأول 2013 [268]، والذي بموجبه حذّر أيٍّ كان من شراء وحيازة واستعمال ما أطلق عليه تسمية "النقود الافتراضية"، وذلك نظراً لمخاطرها العديدة، خصوصاً لناحية تسهيلها لنشاطات اجرامية خاصة بتمويل الإرهاب. ولقد أصدرت هيئة الأسواق المالية إعلاناً مماثلاً بحيث كررت في متن الإعلام رقم 30 تاريخ 12 شباط 2018 [269]، فيما خص تسهيل هذه العملات عمليات تمويل الإرهاب.

وإن حاكم مصرف لبنان رياض سلامة أدلى مراراً بأن العملات التشفيرية تساهم في تمويل الإرهاب[270]، مصرحاً بأن المصرف المركزي رفض استعمال العملات التشفيرية كوسيلة دفع نظراً لكونها سلعة وليست عملة، ولافتقار وجود جهة رقابية أو إشرافية تُعنى بإدارتها.

ولكن، يعدّ أبرز تعديل والذي سنتناوله بالتفصيل، تعديل المادة 316 مكرر من قانون العقوبات بموجب القانون رقم 77 تاريخ 27 تشرين الأول 2016 [271]، بعد انضمام لبنان إلى الاتفاقية الدولية لقمع تمويل الإرهاب لسنة 1999 بموجب القانون رقم 2015/53، ولكن مع إبداء التحفظ على الفقرة (ب) من البند الأول من المادة الثانية من الاتفاقية والتي تنص على تعريف جرم الإرهاب.

فوُضع تعديل المادة 316 مكرر سنداً إلى الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة سنة 1998، والتي انضم اليها لبنان في العام 1999 بموجب القانون رقم 57. فأتى النص الجديد على النحو التالي:

---

[268] مصرف لبنان، اعلام رقم 900 تاريخ 19 كانون الأول 2013 موجه للمصارف وللمؤسسات المالية ولمؤسسات الصرافة ولمؤسسات الوساطة المالية وللجمهور، https://www.bdl.gov.lb/news/more/5/111/65

[269] هيئة الأسواق المالية، اعلام رقم 30 تاريخ 2018/2/12، الجريدة الرسمية، عدد 8 تاريخ 22 شباط 2018، ص. 1105 (المخاطر المتعلقة بالنقود الإلكترونية).

[270] كلمة حاكم مصرف لبنان الأستاذ رياض سلامه خلال ملتقى مكافحة الجريمة الإلكترونية الرابع **4th Anti–Cybercrime Forum**، في فندق فينيسيا، بيروت، 29 تشرين الثاني 2018.

[271] قانون رقم 77 تاريخ 2016/10/27، الجريدة الرسمية، عدد 52 تاريخ 2016/11/3، الصفحات 3473–3474 (تعديل المادة 316 مكرر من قانون العقوبات).

"كل من يقوم أو يحاول القيام أو يوجه أو يشترك عن قصد وبأية وسيلة، مباشرة أو غير مباشرة، بتمويل كلياً أو جزئياً أو المساهمة بتمويل الإرهاب أو الأعمال الإرهابية، أو تمويل شخص إرهابي أو الجماعات الإرهابية، أو الأعمال المرتبطة بها، بما فيها تقديم أو توفير أو جمع الأموال المنقولة أو غير المنقولة، من مصادر مشروعة أو غير مشروعة، في لبنان أو في الخارج، سواء استعملت الأموال أم لم تستعمل، وسواء تم العمل الإرهابي أو لم يتم في لبنان أو في الخارج.

تشمل جريمة تمويل الإرهاب السفر، محاولة السفر، التجنيد، التخطيط، الإعداد، التنظيم، التسهيل، المشاركة، تقديم أو تلقي التدريب، وأي عمل آخر مرتبط بها بنية القيام بأعمال إرهابية ودون ان تكون تلك الأعمال مرتبطة بعمل إرهابي محدد.

يعاقب مرتكبو الأفعال المحددة أعلاه بالأشغال الشاقة المؤقتة لمدة لا تقل عن ثلاث سنوات ولا تزيد عن سبع سنوات وبغرامة لا تقل عن مثل المبلغ المدفوع ولا تزيد عن ثلاثة أمثاله، ولا يحول ذلك دون تطبيق العقوبات المنصوص عليها في المواد 212 لغاية 222 ضمناً من قانون العقوبات".

لا شك بأن هذا التعديل قد وسّع تعريف ونطاق جريمة تمويل الإرهاب، والتي أصبحت تتمتع بخصائص عديدة أبرزها:

-شمول النص للمحاولة الجرمية،

-اعتبار الجريمة بالقصدية وتتألف من القصد العام والقصد الخاص،

-عدم اقتصاره على التمويل والمساهمة الكلية فقط بل الجزئية أيضاً،

-استحداث فعل تمويل الإرهاب الفردي،

-لم يحصر النص نطاق الوسائل التي تقترف بها الجريمة، الأمر الذي يضفي طابع المرونة على عليه ويجنّب اللجوء إلى التفسير أو القياس،

-لناحية مصدر الأموال، لم يفرق بين المصادر المشروعة وغير المشروعة على عكس جريمة تبييض الأموال التي تستوجب ان تكون الأموال من مصدر غير مشروع،

-الصلاحية المكانية للنص تشمل الجرم المقترف في لبنان أم خارجه، إذ تخضع للصلاحية الاقليمية أو الذاتية حسب مكان انطلاقها[272].

-استقلالية فعل تمويل الإرهاب عن جريمة الإرهاب لجهة عدم اشتراط تحقق استعمال الأموال في العمل الإرهابي،

-تجريم التمويل المعنوي للإرهاب المتمثل بالسفر أو محاولة السفر أو التجنيد أو التخطيط أو الإعداد أو التنظيم أو التسهيل أو المشاركة أو تقديم أو تلقي التدريب،

وأي عمل آخر مرتبط بها بنية القيام بأعمال إرهابية ودون ان تكون تلك الأعمال مرتبطة بعمل إرهابي محدد، على ان لا يحصر تطبيق النص بهذه الوسائل فقط.

-لم يطرأ أي تعديل على العقوبة، فبقيت العقوبة بتلك السالبة للحرية المتمثلة بالأشغال المؤقتة لمدة لا تقل عن ثلاث سنوات ولا تتعدى السبع سنوات، إضافة إلى العقوبة المالية النسبية وهي الغرامة التي لا تقل عن مثل المبلغ المدفوع ولا تزيد عن ثلاثة امثاله.

من الملاحظ بأن لبنان وباستثناء تعاميم مصرف لبنان وهيئة الأسواق المالية التحذيرية، يفتقر إلى أي صك قانوني أو نص قانوني يجرم أو يلحظ تجريم تمويل الإرهاب عبر العملات التشفيرية، أو يفرض قواعد تخضع إليها خصيصاً المؤسسات المالية لناحية سبل اقتفاء أو الكشف عن عمليات تمويل الإرهاب بواسطتها. ففي غياب النص، تطرح اشكالية مدى انطباق المادة 316 مكرر لعملية تمويل الإرهاب عبر العملات التشفيرية.

إن المادة 316 مكرر عددت طرقاً مادية ومعنوية تساهم مباشرة أو غير مباشرة في عملية تمويل الإرهاب. ولا مندوحة بأن هذه الوسائل قد وردت بدون شك على سبيل المثال لا الحصر، والدليل على ذلك استعمال

---

[272] د. سمير عالية، **الجرائم الواقعة على أمن الدّولة الخارجي والدّاخلي**، منشورات الحلبي الحقوقية، الطبعة الأولى، 2019، ص. 342.

المشرع عبارة "بما فيها" قبل تعداد بعضاً من هذه الوسائل، الأمر الذي يجعل هذا النص مرناً وغير مقيّد ومحصور من ناحية التطبيق.

بالإضافة إلى ذلك، ولعل الدليل الأكبر لمرونة النص وعدم اقتصاره بما هو مذكور، هي عبارة "وبأية وسيلة" التي وردت في بداية النص، فهكذا جرّم المشرع اللبناني فعل تمويل الإرهاب بغض النظر عن الوسيلة أو الطريقة التي بموجبها اقترف الفعل.

برأينا، إن مرونة نص المادة 316 مكرر خصوصاً لناحية عدم تقييد الوسائل، تفسح المجال لتطبيقها على أفعال تمويل الإرهاب المرتكبة من خلال أو بواسطة العملات التشفيرية، طبعاً في حال تحقق سائر الأركان والعناصر المتطلبة لقيام الجرم. ولكن من الناحية التطبيقية، لا بد التطرق إلى مدى امكانية تجميد العملات التشفيرية وفقاً للفقرة الثالثة [273] من المادة 6 من القانون رقم 2015/44. فالفقرة الثالثة منحت هيئة التحقيق الخاصة الحق الحصري بتقرير "التجميد النهائي للحسابات و/أو العمليات المعنية... التي يشتبه بأنها تتعلق بتبييض أموال أو بتمويل ارهاب" على غرار حق الهيئة بتقرير إبقاء أي حساب مشتبه به قيد المتابعة والمراقبة (**Traceable**). فهل يمكن تطبيق هذا التجميد على حسابات أو سائر انواع المحفظات التي تتضمن عملات تشفيرية مشبوهة؟ (بغض النظر عن الامكانية التقنية) وعلى جميع الأحوال، كيف يمكن لهذه الحسابات أن تبقى قيد المتابعة؟ باختصار، الإجراءات التي تخضع لها المصارف والمؤسسات المالية لهذه الناحية لا تسرِ في الوقت الراهن على العملات التشفيرية.

وبناءً عليه، أي قوانين وأي إجراءات ستخضع لها عملة لبنان الرقمية المنوي إطلاقها؟

---

[273] تنص الفقرة الثالثة من المادة 6 من قانون 2015/44 على ما يلي:

"يُحصر «بالهيئة»، بعد اجراء التدقيق والتحليل اللازمين، حق تقرير:

– التجميد النهائي للحسابات و/أو العمليات المعنية و/أو رفع السرية المصرفية لصالح المراجع القضائية المختصة ولصالح الهيئة المصرفية العليا بشخص رئيسها عن الحسابات او العمليات التي يشتبه بأنها تتعلق بتبييض أموال أو بتمويل الإرهاب.

– إبقاء الحسابات المشتبه بها قيد المتابعة (Traceable) لـ«الهيئة» الرجوع، بشكل نهائي أو كلي، عن أي قرار تتخذه وذلك في حال توفرت لديها معطيات جديدة بهذا الخصوص."

انطلاقاً من هنا وفي ظل النقص في النصوص التشريعية في مجال مكافحة مويل الإرهاب الحديث، ننتقل إلى النطاق العلوي السيبراني والذي ينكل بدوره للتنظيم القانوني والنصوص القانونية خصوصاً على صعيد قانون العقوبات.

الباب الثاني: الجرائم السيبرانية

فكرة الجريمة السيبرانية ليست بالجديدة، ولكن هناك ارتباك كبير ينتاب الأكاديميين والتقنيين والقانونيين حيال نطاق هذه الجريمة وتعريفها، فليس هناك من تعريف موحّد.

يمكن تعريف الجريمة السيبرانية على أنها "أي جريمة يتم تسهيل ارتكابها أو تُرتكب بواسطة الحاسوب أو الشبكة أو جهاز إلكتروني"[274]. قد يكون الحاسوب أو الجهاز هو "مرتكب" الجريمة، أو مسهّلها أو الهدف بحد ذاته.

تطوّرت الجرائم السيبرانية على مدار السنين، ولا تزال في طور التبلور والنضوج والانتشار تماشياً مع التكنولوجيا الحديثة بحيث تحوّل تركيز مرتكبيها يوماً بعد يوم إلى أهدافٍ أجلّ وأكثر ربحاً. فباختراع برامج وأجهزة مستحدثة تظهر جرائم وأفعال جديدة تستهدف هذه التقنيات الحديثة، الأمر الذي يشكّل حاجزاً أمام سلطات إنفاذ القانون والمشرّعين.

ومع ظهور العملات التشفيرية الكائنة في نموذج رقمي، كان من الطبيعي أن تُستهدف وتُستغل هذه العملات في الجرائم السيبرانية، لا بل ظهرت جرائم وأفعال غير مشروعة لم تكن كائنة مسبقاً.

لذلك ارتأينا مناقشة أبرز هذه الجرائم في فصلين، الأول يتمحور حول البرمجيات الخبيثة والثاني يعالج التقليد الرقمي والإنفاق المضاعف.

[274] Sarah Gordon, and Richard Ford. "On the definition and classification of cybercrime." Journal in Computer Virology, Vol. 2.1, 2006, pp. 13-20, p. 14.

الفصل الأول: الأفعال المرتكبة عبر البرمجيات الخبيثة

البرمجية الخبيثة **Malware (Malicious Software)** أو برنامج حاسوب خبيث، هو برنامج يُصيب الجهاز الإلكتروني من خلال البريد الإلكتروني أو المواقع الإلكترونية أو الأجهزة الخارجية المتصلة. يتم استخدام هذا البرنامج للاستيلاء على الأجهزة الإلكترونية، وتحويلها إلى أجهزة "زومبي" قد يتم استغلالها كجزء من شبكة الروبوتات **Botnets** تُستعمل لإرسال الرسائل غير المرغوب بها **Spam** أو تنفيذ هجمات حجب الخدمة عن مواقع. غالباً ما يكتشف مالك الجهاز المُصاب بواقعة إصابة جهازه، جرّاء تباطؤه تدريجياً أو عدم قدرته من إزالة برنامج غير قابل للتمييز. من أبرز أنواع هذه البرمجيات نذكر الفيروسات وأحصنة الطروادة **Trojan** وبرامج التجسس...

في السنوات الأخيرة، انبثق وانتشر نوعان من البرمجيات الخبيثة اكتسحتا العالم وأحدثتا أضراراً في العديد من القطاعات، هما الرانسوم وير **Ransomware** والكريبتوجاكينغ **Cryptojacking**. فما علاقتهما بالعملات التشفيرية؟

سنبحث العلاقة مع الرانسوم وير في المبحث الأول لننتقل إلى العلاقة مع الكريبتوجاكينغ في المبحث الثاني.

المبحث الأول: الفدية الإلكترونية Ransomware

تُعدّ هجمات الفدية الإلكترونية رانسوم وير **Ransomware**، من الأكثر انتشاراً ورواجاً في حقل الجرائم السيبرانية في الأعوام الماضية. يمكن تعريف الرانسوم وير أو فيروس الفدية على أنه نوع من البرمجيات الخبيثة **Malware** التي تخترق الجهاز الإلكتروني وتمنع المستخدم من الولوج إلى الأنظمة أو الملفات التابعة له.

عندما يُصاب جهاز معين ببرمجية الرانسوم وير، يتحوّل بكامله أو بعض الملفات المستهدفة إلى رهينة بيد المجرم السيبراني، بحيث يلجأ هذا الأخير إلى استخدام التشفير لمنع الولوج إلى الجهاز أو الملف المشفّر وذلك لحين تسديد الضحية الفدية المطلوبة خلال فترة زمنية محدودة. وكنتيجة، في حال رضخت الضحية لهذا الابتزاز وسددت الفدية، تحصل على مفتاح فك التشفير الذي يمكّن من الولوج مجدداً إلى النظام أو الملفات محل موضوع التشفير. ولكن إذا تمنّعت الضحية عن الخضوع لرغبات الفاعل، آنذاك يعمد المجرم إلى تسريب البيانات أو محوها أو تعطيل الجهاز بكامله...

في غالب الأحيان، يُصاب الجهاز بفيروس الرانسوم وير عبر الملحقات والروابط الخبيثة الملحقة برسائل البريد الإلكتروني المعروفة بالتصيّد الإلكتروني **Phishing Emails**، وهي إحدى الطرق الشائعة لتحميل برنامج رانسوم وير إلى الجهاز حيث يُصاب الجهاز بمجرد نقر المستخدم للرابط أو الملحق. أما الطريقة الثانية المعتمدة لنشر الرانسوم وير فتسمى بالـ **Drive-by downloading** حيث يتم تحميل البرنامج الخبيث على الجهاز بعد زيارة المستخدم موقعاً إلكترونياً مصاباً. في معظم الأوقات لا يكون القائم على الموقع المُصاب هو وراء البرنامج أو حتى على معرفة من الأمر، فمرسلي البرنامج يستهدفون المواقع ذات الأمن الضعيف والفجوات التي تمكّنهم من اختراقها وإصابتها... فنكون أمام ضحيتين، الأولى هي المواقع الإلكترونية والثانية المستخدم الزائر للموقع.

تُعد هذه الهجمات وسيلة ابتزاز وتهديد بامتياز ذات الأهداف المادية، وتلحق اضراراً فادحة سواء على الصعيد الشخصي أو على صعيد القطاعين العام والخاص وخسائر مالية وساعات عمل وانتاج، ناهيك عن الضرر المحتمل لسمعة المؤسسة المستهدفة.

تاريخياً، سُجّلت أول هجمة فدية خبيثة في العام 1989 وعُرفت بـ "حصان طروادة مرض الإيدز" **AIDS Trojan** التي انتشرت أنحاء تسعين دولة وذلك عبر توزيع عشرين ألف قرص مرِن **Floppy**

Disks، بعد أن أرسلها جوزيف بوب **Joseph Popp** العالم في جامعة هارفارد، إلى مؤتمر منظمة الصحة العالمية حول مرض الإيدز[275].

تطوّرت على مر السنوات أوجه وطرق ارتكاب هجمات الفدية الإلكترونية، وأنه يمكن تصنيفها إلى نوعين[276]:

الأول المعروف بـ **Locker Ransomware** وهو عبارة عن برنامج حظر يمنع ويقيّد الولوج إلى نظام الحاسوب أو الجهاز بكامله دون المساس بالنظام الأساسي أو البيانات المخزنة، بحيث يجعل الجهاز غير قابل للاستخدام.

النوع الثاني معروف بـ **Crypto Ransomware** وهو عبارة عن برنامج تشفير يمنع الولوج والوصول إلى البيانات والملفات التي يستهدفها مرسِل البرنامج، لا يمس أو يعطّل الجهاز بكامله أي أنه موضعي.

يعتبر النوع الثاني أي الـ **Crypto Ransomware** الأكثر رواجاً، فهو مُصمَم للتنقيب والعثور على البيانات القيّمة المخزنة داخل الجهاز ليقدم آنذاك على تشفيرها بحيث تصبح البيانات أو الملفات المستهدفة عديمة الفائدة جراء التشفير، وذلك طبعاً لحين دفع الفدية واستحصال المستخدم لمفتاح فك التشفير وتبعاً استرجاع حق الولوج. تختلف هذه البيانات والملفات المستهدفة، فمنها شخصية كالصور والفيديوهات ومشاريع جامعية ومنها ملفات فائقة الأهمية وذات الطابع السري تابعة للقطاعين العام والخاص مثل بيانات وملفات القطاع الصحي أو الأمن الداخلي إلخ.

في طبيعة الحال، إن آلية الدفع المعتمدة هي تلك الإلكترونية طبعاً، ولكن سرعان ما استُبدلت وسائل الدفع هذه بالعملات التشفيرية التي أضحت طريقة الدفع المحببة والفدية المطالب مع الجيل الجديد

---

275 Alina Simone. “The Strange History of Ransomware.” Medium, 26 Mar. 2015, medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b, Accessed 28 Sept. 2018.

276 Symantec. Annual Report on **The evolution of ransomware**, Version 1.0, 6 Aug. 2015, www.symantec.com, Accessed 7 Sept. 2018.

من هجمات الـ **Crypto Ransomware** [277]. أما بالنسبة إلى آلية الدفع عن طريق العملات التشفيرية، فهي شبيهة بوسائل الدفع الإلكترونية بحيث بعد نجاح البرمجية من اختراق نظام الجهاز وتشفير الملفات والبيانات، تظهر على الشاشة رسالة إشعار تُعلم المستخدم بأنه وقع ضحية الهجمة ويُهدد بمسح بياناته نهائياً أو تعديلها أو تسريبها إذا لم ينصاع ويدفع المقدار المعين من العملة التشفيرية.

كان من الطبيعي أن تتصدر البيتكوين قائمة العملات الأكثر مطالب بها كفدية خصوصاً في الآونة الأخيرة مع ارتفاع سعرها. وتفادياً لأية تعقيدات ناتجة عن جهل أو عدم المام بعض الضحايا بطرق التعامل مع البيتكوين، فلقد درجت العادة أن تُرفق رسالة الابتزاز بروابط أو معلومات تشرح بالتفصيل كيفية شراء وإرسال البيتكوين.

لا شك من أن الخصائص التي تتمتع بها العملات التشفيرية هي من إحدى العوامل التي تزيد من نسبة هذه الهجمات. فميزة المجهولية واللامركزية تسمحان للمجرم الحصول على العملات التشفيرية من الضحايا مباشرة، دون المرور عبر المؤسسات المالية كالمصارف التي تسمح بتعقّب المعاملات كافة، مسهّلة وظيفة الشرطة وأجهزة الملاحقة من الوصول إلى المجرم[278].

بات الأفراد والشركات والمصارف والمؤسسات التعليمية والمستشفيات والهيئات الحكومية في السنوات الأخيرة رهائن نتيجة الأجيال الجديدة من الـ **Crypto Ransomware** والتي تزداد تعقيداً من الناحية التقنية، سواء لجهة تطورها وقدرتها لتفادي احتمالات فشل الهجمة أو لجهة تغلبها على أية تعقيدات تشكّل عائقاً أمام تحصيل الفدية.

---

[277] ibid. p. 23.

[278] Tom Keatinge, et al. Study commissioned by European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, on "**Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses: Counter-terrorism**," No. PE 604.970, May 2018, p. 38.

تاريخياً كانت برمجيات **TeslaCrypt** و**Locky** و**CryptoWall** من أول الهجمات التابعة للجيل الجديد من الفدية الإلكترونية التي يطالب بموجبها مرسِل البرمجية تسديد الفدية بالعملات التشفيرية. ولعلّه كانت هجمة الـ **WannaCry** التي ظهرت في شهر أيار من العام 2017، من أكثر الهجمات انتشاراً وذات النطاق الجغرافي الواسع بحيث أصابت حوالي ثلاثمائة ألف حاسوب على امتداد مئة وخمسين دولة[279]، وكلّفت المستخدمين آلاف الدولارات من أموال الفدية والمليارات جراء ساعات الإنتاجية المفقودة. شلّت هذه الهجمة القطاع الصحي البريطاني وطالت وزارة الداخلية الروسية والعديد من القطاعات العامة والخاصة. طالب المبتزّون من كل ضحية تسديد مبلغ يتراوح بين الـ 300 و600 دولار أمريكي من البيتكوين، وتجلّت آلية الدفع عبر ارسال المبالغ المطلوبة إلى إحدى عناوين البيتكوين المذكورة ضمن رسالة التشفير الظاهرة على شاشة الحاسوب. ونتيجةً لعملية التعقّب والتتبع الممكنة عبر شبكة البلوكشاين، أفادت بعض التقارير أنه في فترة لاحقة تم تحويل كمية البيتكوين المكتسبة جراء هذه الهجمة إلى عملة مونيرو **Monero** (**XMR**) عبر منصة تبادل سويسرية، وذلك طبعاً كوسيلة لتبييض الأموال[280] وتضليل المصدر الأساسي للعملات.

نذكر قضية أخرى بيّنت السلبيات والمخاطر الناتجة عن الحكومة الإلكترونية والتحول الرقمي الجذري لدى الإدارات العامة، الذي أدى إلى الاستغناء عن المستندات الورقية إلخ. فأُفسح المجال أمام المجرم السيبراني لإثبات قدراته على السيطرة وفرض الاحتلال الرقمي لدولة أو مدينة كاملة... تبلورت

[279] Russell Goldman. “What We Know and Don't Know About the International Cyberattack.” The New York Times, 12 May 2017, www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html, Accessed 23 Sept. 2018.

[280] William Suberg. “Bitcoin Exchange ShapeShift Helps Police as WannaCry Attacker Converts to Monero.” Cointelegraph, 4 Aug. 2017, cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero, Accessed 22 Sept. 2018.

الحادثة في مدينة بالتيمور الأميركية، التي تعرّضت لهجمة أُطلق عليها اسم روبين هود، والتي شلّت المؤسسات العامة عبر تشفير الملفات لقاء فدية مالية بقيمة مئة ألف د.أ. تُسدد بالبيتكوين[281].

– **تقنية البلوكشاين وسيلة لدرء الهجمات؟**

يرى البعض[282] بإمكانية الانتفاع من تقنية البلوكشاين كآلية دفاع بوجه هجمات الفدية الإلكترونية. تكمن الفكرة بإمكانية حفظ المعلومات الحساسة على شبكة البلوكشاين بطريقة لامركزية، على عكس الأنظمة المركزية الراهنة لحفظ المعلومات. فتخزين وحفظ المعلومات بطريقة غير مركزية تعيق ربط وإسناد معلومة معينة إلى صاحبها، وبالتالي من العسير أيضاً تحديد الجهة المعنية والمرجوّة لتوجيه البرمجية الخبيثة. بالإضافة إلى ذلك، تمكّن طبيعة البلوكشاين من إنشاء نسخ غير محدودة من المعلومة عينها، الواقعة التي تجعل فكرة "حجز" نسخة من ملف لقاء فدية والتهديد بتعديله أو مسحه بالأمر السخيف... وإن علانية سجل البلوكشاين يؤلف عاملاً رادعاً اضافياً أمام المجرم[283].

إن هجمات الرانسوم وير في عداد الهجمات المتوقع لها مستقبلاً مرموقاً. فكلما انتشرت الأجهزة الإلكترونية، كلما اتّسع نطاق هذه الهجمة، وبالتالي ضوعف الضرر وتكاثر عدد الضحايا وارتفعت نسبة الخسائر.

---

281 Joe Pinkstone. “RobinHood Ransomware Attack That Paralysed Baltimore's Government Could Be Coming to YOUR City.” Daily Mail Online, Associated Newspapers, 29 May 2019, www.dailymail.co.uk/sciencetech/article-7082001/RobinHood-ransomware-attack-paralysed-Baltimores-government-coming-city.html, Accessed 8 Jun. 2019.

282 Emerging Technology from the arXiv. “True Scale of Bitcoin Ransomware Extortion Revealed.” MIT Technology Review, 19 Apr. 2018, www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/, Accessed 18 Sept. 2018.

283 Tom Serres. “2017's Ransomware Attacks: Could Blockchain Technology Have Prevented Them?”, Medium, 30 May 2017, medium.com/animal-meia/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b, Accessed 17 Sept. 2018.

لا مندوحة بأن الاعتماد التصاعدي على التكنولوجيا والتحول الرقمي، انعكس سلباً وتحوّل إلى عامل تحفيزي لازدياد كافة الهجمات السيبرانية وبالأخص الفدية الإلكترونية، واللجوء إلى المدن والبيوت الذكية التي تستند بكافة نواحيها على أجهزة إنترنت الأشياء تزيد من فرص تعرضها وتحويلها إلى رهينة بيد المجرم السيبراني. فلعله من السليم قبل استبدال البنى التحتية الراهنة والاستغناء عن التقنيات القديمة بالحديثة، وضع خطط واستراتيجيات دفاع للأمن السيبراني تحصّن بها سائر القطاعات وذلك كنهج استباقي. وإن اتخذ إجراءات كهذه تحدّ أيضاً من ظاهرة التعدين غير المشروع **Cryptojacking**.

المبحث الثاني: الكريبتوجاكينغ CryptoJacking

استقطبت المجرم السيبراني فكرة تحصيل عملات تشفيرية ذات قيمة عبر عملية التعدين. فوجد فيها طريقة لاستعباد أجهزة الغير الإلكترونية لتحقيق مكاسبه المالية من دون تكلفة، وذلك عن طريق استحداث فعل جديد بطبيعته وهو التعدين غير المشروع **Illicit Cryptomining** عبر برمجية خبيثة والمسمى بالكريبتوجاكينغ **CryptoJacking**.

يمكن تعريف فعل الكريبتوجاكينغ بالاستخدام السري وغير المصرّح به لأجهزة الغير الإلكترونية من حواسيب وهواتف ذكية (وأي جهاز من فئة إنترنت الأشياء) بهدف تعدين عملات تشفيرية. يُعدّ هذا الفعل نوع من أنواع الولوج غير المشروع والسرقة، لأن الفاعل يعمد إلى سلب قوة معالجة الجهاز الخاص بالضحية ووحدة المعالجة المركزية **Cloud CPU Usage** لتعدين العملات التشفيرية بعد الولوج غير المصرّح إلى الجهاز، أي دون علم أو إرادة صاحب الجهاز.

يتجلّى هدف هذا الفعل بالمردود المادي المتمثل باستخراج وتجميع عملات تشفيرية قيّمة دون تكبّد المصاريف أو تبوّأ العواقب. يتفادى الجاني كلفة اقتناء أجهزة إلكترونية للتعدين؛ ويتحاشى تسديد فواتير

الكهرباء المرتفعة نتيجة استهلاك عملية التعدين المستمرة كميات هائلة من الطاقة، والتي في نهاية المطاف تسددها الضحية صاحبة الجهاز المُستعبد.

نذكّر أن عملية التعدين بحد ذاتها قانونية ومشروعة، إلا أن فعل الكريبتوجاكينغ هو بالفعل غير مشروع. ما يميّز فعل التعدين غير المشروع عن سائر جرائم العملات التشفيرية، بأن الضحية في أغلب الأوقات لا تكون من المتعاملين أو من أصحاب العملات التشفيرية حتى[284].

تقنياً، هناك وسيلتان تمكّنان اقتراف التعدين غير المشروع، وهما التعدين القائم على ملف والتعدين القائم على المتصفح[285] وسنبحثهما تبعاً:

الطريقة الأولى المتمثلة بالتعدين القائم على ملف أي الـ **File-Based Coin Mining**، تُشغَّل مثل البرمجيات الخبيئة. أما عن كيفية وصول الملف الخبيث إلى الجهاز فهناك طرق عديدة وبسيطة، أبرزها الروابط الإلكترونية الخبيثة المزروعة على شبكة الإنترنت وبالأخص تلك المرفقة بالرسائل الإلكترونية، سواء المتضمنة في البريد الإلكتروني أو في الرسائل المرسلة عبر تطبيقات التحادث مثل الواتساب والفايسبوك مسنجر. يتم تحميل الملف الخبيث ورمز التعدين مباشرةً على الجهاز بمجرّد نقر الضحية على الرابط. وتبعاً، يعمد الجهاز إلى تشغيل عملية التعدين في الخلفية خفيةً وعلى على مدار الساعة طبعاً من دون علم أو إرادة صاحبه. إن هذه الوسيلة المحلية تحوّل كامل الجهاز المُصاب الى رهينة دائمة بيد مرسلي البرنامج الخبيث ومصدر ثابت لجباية العملات التشفيرية.

الطريقة الثانية المتمثلة بالتعدين القائم على المتصفح **Browser-Based Coin Mining** وهي الأكثر شيوعاً، تعتمد على استغلال الإعلانات الإلكترونية أو المواقع ذات الأمن الضعيف لزرع برامج

---

[284] Symantec. "What is cryptojacking? How it works and how to help prevent it." Norton, https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html, Accessed 3 Nov. 2018.

[285] Symantec. Internet Security Threat Report on **Cryptojacking: A Modern Cash Cow**, September 2018, p. 3, www.symantec.com, Accessed 3 Oct. 2018.

خبيثة. يتضمن المخطط تضمين جزء من نص **JavaScript** في موقع إلكتروني معيّن، والذي بدوره يمكّن من تحويل الجهاز إلى معدِّن عملات تشفيرية بمجرد زيارة الضحية لهذا الموقع. يباشر البرنامج النصي المذكور بالعمل في الخلفية ويمكّن سرقة قوة المعالجة لجهاز الحاسوب أو الهاتف الذكي الخاص بالزائر، وطبعاً من دون علمه وإرادته. من الملفت هنا أن العديد من المواقع المضيفة للبرامج الخبيثة أصحابها يجهلون استضافة موقعهم لهكذا برنامج ورمز، فنكون أمام ضحيتين وهما الموقع بحد ذاته وزائر هذا الموقع. في المقابل يعمد البعض الآخر من أصحاب المواقع إلى استضافة البرامج المعدّنة برضاهم وعن قصد، فالأكثرية لا يُعلمون الزائر بذلك. في المقابل هناك أقلية تقوم على إعلام الزائر بذلك نظراً لطبيعة الموقع بحد ذاته الذي يكون من البداية مُخصص للتعدين، فالزائر يكون قاصداً زيارة الموقع بهدف جعل جهازه جهازاً معدّناً.

من المفاعيل والنتائج السلبية للتعدين غير المشروع نذكر:

تباطؤ الجهاز، ارتفاع درجة حرارة البطاريات، زيادة استهلاك الطاقة، انخفاض الانتاجية لدرجة جعل الأجهزة غير صالحة للاستعمال. وعلى صعيد المؤسسات بصورة خاصة، يؤدي التعدين غير المشروع إلى استنزاف الموارد وزيادة عبء العمل وخطر إحداث الأضرار المادية على البنية التحتية لتكنولوجيا المعلومات، مما يسبب زيادة كلفة الكهرباء بشكل هائل، وخفض إنتاجية العمليات التجارية التي تعتمد على الطاقة الحاسوبية. وبالتالي، وعلى عكس الرانسوم وير، لا يشلّ التعدين غير المشروع الجهاز بأكمله ولا يحتجزه كرهينة عن بُعد ولا يُقيّد الوصول إلى النظام أو البيانات عبر تشفيرها، بل يبقى الجهاز قابلاً للاستعمال.

يهدد الكريبتوجاكينغ بصورة عامة الأمن السيبراني على الصعيدين المؤسساتي والفردي، وإن قيام واكتشاف تعدين غير مشروع داخل مؤسسة معينة يُعتبر من المؤشرات الدالة لوجود عيوب وفجوات كبيرة في أنظمتها السيبرانية[286].

[286] Cyber Threat Alliance. Report on **The Illicit Cryptocurrency Mining Threat**, September 2018, p. 4, https://www.cyberthreatalliance.org/resources/, Accessed 11 Nov. 2018.

أما على صعيد الأرقام والإحصاءات، تكشف الدراسات بأن وتيرة ورواج التعدين غير المشروع بدأ يتخطى ويستبدل جريمة الابتزاز الإلكتروني الرانسوم وير[287]. ولقد وجد الباحثون أن العملة التشفيرية مونيرو **Monero** هي العملة الأكثر شعبية لدى المجرمين فوفقاً لدراسة أُجريت في العام 2019، إن أكثر من 4.3 في المئة من عملة مونيرو المتداولة في السوق هي نتيجة أنشطة إجرامية[288]. وعلى وجه التحديد، تكشف البيانات التي جمعتها شركة **Palo Alto Networks** [289] في تموز سنة 2018 بأن عملة مونيرو تشكّل 85 في المئة من العملات المعدّنة عبر البرمجيات الخبيثة، تليها البيتكوين بنسبة 8 في المئة وسائر العملات التشفيرية 7 في المئة فقط[290].

رغم أن قيمة عملة مونيرو أدنى بكثير من قيمة البيتكوين[291]، إلا أنها تتصف بعوامل تجعلها مرغوبة من قبل المجرم السيبراني خصوصاً لجهة ميزة الخصوصية الفائقة وخاصية المجهولية التامة التي توفرها. هذه عوامل تساهم من إخفاء أنشطة التعدين وحركة المعاملات الجارية عبر هذه العملة، بحيث يتم إخفاء العناوين وحركة المعاملات تلقائياً دون الحاجة إلى برامج أو أدوات خارجية كعملة البيتكوين مما يعني انعدام قابلية تتبع الأثر الرقمي. بالإضافة إلى ذلك، الموارد المطلوبة لاستخراج وتعدين عملة مونيرو ليست بالباهظة والمعقّدة، الأمر الذي يسمح باستهداف الحواسيب الشخصية التي لا تتمتع بقوة معالجة عالية نسبياً ويسبب تبعاً إلى ارتفاعٍ في عدد الأهداف المحتملة.

---

[287] Kaspersky Lab. Annual report on **Ransomware and Malicious Cryptominers 2016-2018**, 27 Jun. 2018, p. 3, www.securelist.com, Accessed 8 Nov. 2018.

[288] Sergio Pastrana, and Guillermo Suarez-Tangil. "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth." Proceedings of the Internet Measurement Conference, 2019, pp. 73-86.

[289] شركة رائدة في الأمن السيبراني، مقرها في ولاية كاليفورنيا الأميركية.

[290] Cyber Threat Alliance. Report on **The Illicit Cryptocurrency Mining Threat**, Op.cit., p. 9.

[291] بتاريخ كتابتنا لهذا الفصل (شهر آب 2019) بلغت قيمة عملة البيتكوين الواحدة /11.900/ دولار أميركي، وفي المقابل بلغت قيمة عملة مونيرو الواحدة /92/ دولار أميركي.

تلعب طبيعة خوارزمية عملة مونيرو دوراً جوهرياً باستقطاب المعدّنين، فهذه الخوارزمية قد تم تصميمها بهدف جذب المستخدمين وتشجيع آخرين للانضمام والمساهمة في الشبكة الخاصة بالعملة؛ الواقعة التي تمكّن من تحقيق المزيد من الأرباح بسبب سهولة امكانية المعالجة عبر الطاقة المسروقة، خصوصاً عن طريق شبكة الروبوتات **Botnets** [292]... كل هذه الخصائص حثّت إلى تعدين عملة مونيرو بدلاً من عملة البيتكوين[293].

من جهة الكشف عن هويات مرتكبي فعل التعدين غير المشروع وملاحقتهم القضائية، تُعتبر سلطات إنفاذ القانون اليابانية أول من استطاع من تعّقب والتوصّل إلى مرتكبي هذا الفعل وعلى احالتهم إلى المراجع القضائية المختصة للمحاكمة. وعليه، سنعرض تبعاً التجربة اليابانية والفرنسية توصلاً إلى مدى إمكانية ملاحقة هذا الفعل في لبنان.

- **التجربة اليابانية في الملاحقة والمحاكمة:**

تُعتبر اليابان من أول الدول التي بدأت بملاحقة مرتكبي فعل التعدين غير المشروع، ولقد سارعت سلطات إنفاذ القانون إلى تعقّب هؤلاء وإحالتهم إلى السلطات القضائية المختصة والتي أصدرت عدة أحكام متنوعة بهذا الشق. ففي حكم مثير للجدل، حكمت محكمة في مدينة يوكوهاما اليابانية ببراءة مواطن كان قد ارتكب فعل التعدين غير المشروع، عبر استخدامه خدمة **Coinhive** [294] على موقعه الإلكتروني ومن

---

[292] البوت نت أو شبكة الروبوت Botnet تسمية مشتقة من عبارة Robot Network هي عبارة عن شبكة مؤلفة من أجهزة إلكترونية من حواسيب وهواتف ذكية وأجهزة إنترنت الأشياء إلخ. تم اختراقها عبر برامج خبيثة وهي مرتبطة ببعضها البعض عبر شبكة الإنترنت. يتم استخدام هذه الشبكة لشن الهجمات الإلكترونية وذلك بناءً لأوامر سيد البوت Master Bot، والذي يدير الشبكة ويتحكّم بالهجمات.

تسهّل البوت نت عملية التعدين غير المشروع وذلك جراء توفيرها قوة معالجة هائلة للتعدين.

[293] Kafeine. "Smominru Monero mining botnet making millions for operators." ProofPoint, 31 Jan. 2018, https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators, Accessed 20 Sept. 2018.

[294] كوين هايف Coinhive هي خدمة عبارة عن برنامج، تجيز للمستخدم ان يعدّن عملة مونيرو المشفرة عبر دمجها بموقعه الإلكتروني.

دون إعلام الزوار بذلك، محوّلاً بذلك جهاز كل زائر إلى جهاز معدِّن مُستعبَد. وفي حيثيات القضية، اعتبرت المحكمة بأن إدانة الفاعل هو بالأمر المفرط والمتطرّف لأن نص البرنامج المستخدم ليس بالفيروس، معتبرةً بأن فعله ليس بالجرم وليس بذاك غير المقبول اجتماعياً[295]. أثار هذا الحكم الجدل، فاستنكر البعض التبرئة جرّاء عدم اعتبار برنامج الـ **Coinhive** بالفيروس، إلا أن آثار هذا الحكم لم يدم طويلاً ففي شهر شباط من العام 2020 أصدرت المحكمة العُليا في طوكيو قراراً قضى بنقضه مغرّمةً المدعى عليه مبلغ وقدره مئة ألف ين ياباني (أي 910 د.أ.)[296].

في المقابل، أدانت محكمة في مدينة سنداي اليابانية وفي أوّل حكمٍ من نوعه، مواطناً اقترف فعل التعدين غير المشروع بطريقة مشابهة لتلك المذكورة أعلاه، فلقد أقدم الفاعل على إدخال النص الخاص ببرنامج **Coinhive** إلى أدوات غش لألعاب إلكترونية. أنزلت المحكمة على الفاعل عقوبة الحبس لسنة واحدة مع تعليق تنفيذها لمدة ثلاث سنوات، وذلك سنداً إلى أحكام قانون منع المنافسة غير المشروعة اليابانية[297].

- **<u>التجربة الفرنسية:</u>**

خلال شهر آب من العام 2019، تمكّنت السلطات الفرنسية المتمثلة بشعبة الشرطة السيبرانية المعروفة بـ **"Cyber Gendarmes"** من رصد وإغلاق شبكة من البوتنت تمكّن القراصنة بواسطتها من

---

295 “Man acquitted over cryptomining program that used site visitors' PCs.” Japan Today, 28 Mar. 2019, https://japantoday.com/category/crime/man-acquitted-over-cryptomining-program-that-used-site-visitors'-pcs, Accessed 5 Apr. 2019.

296 “Japan court convicts man of installing cryptomining programs without consent,” The Mainici, 7 Feb. 2020, https://mainichi.jp/english/articles/20200207/p2g/00m/0dm/083000c, Accessed 13 Feb. 2020.

297 Kevin Helms. “Japan Gives Jail Sentence to Crypto Miner in a Remote Mining Case.” Bitcoin News, 3 Jul. 2018, news.bitcoin.com/japan-jail-sentence-crypto-miner-remote-mining/, Accessed 27 Sept. 2018.

نشر فيروس **Retadup** على أكثر من 850.000 جهاز حاسوب موزّع ضمن مئة دولة. لقد أوضحت الشرطة الفرنسية بأن هدف الفيروس هو تحويل الأجهزة المُصابة إلى أجهزة تعدين لعملة مونيرو التشفيرية[298].

أما في لبنان، فطبعاً ليس هنالك من نصٍ قانوني خاص يتطرّق إلى التعدين غير المشروع، ولكن إذا ما تواجدت المحاكم اللبنانية يوماً ما أمام قضية كهذه، فجلّ ما يمكن أن تحكم به هو جنحة المادة 110 من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي[299] المتمثل بفعل الولوج غير المشروع إلى نظام معلوماتي. فهذه المادة يمكن تطبيقها على الشق الأول من فعل التعدين غير المشروع والمتمثل باختراق وولوج البرنامج الخبيث إلى الجهاز بطريقة غير مشروعة.

من جهة أخرى، عبر تشريح فعل التعدين غير المشروع، يتبين أن الشق الثاني منه يتكون من سرقة طاقة المعالجة للجهاز واستغلاله لمكاسب الفاعل الشخصية. وإذا ما راجعنا النصوص المتعلقة بفعل السرقة التقليدي، نرى أن المشرّع اللبناني قد جرّم في الفقرة الثانية من المادة 635 من قانون العقوبات فعل سرقة الطاقة المحرزة بحيث أتى في حرفيته "تنزل الطاقات المحرزة منزلة الأشياء المنقولة في تطبيق النصوص الجزائية"، فهل من مجال لتوسيع تفسير هذا النص ليشمل طاقة المعالجة الخاصة بالأجهزة الإلكترونية في ظل غياب نص خاص؟ فجريمة السرقة تحوّلت من سرقة مادية سواء بالكسر والخلع أو استخدام السلاح

---

298 “La gendarmerie a neutralisé un réseau de 850 000 ordinateurs infectés par le même virus,” Le Monde, 28 Aug. 2019, https://www.lemonde.fr/pixels/article/2019/08/28/la-gendarmerie-a-neutralise-un-reseau-de-850-000-ordinateurs-infectes-par-le-meme-virus_5503771_4408996.html, Accessed 26 Oct. 2019.

299 تنص المادة 110 من القانون رقم 2018/81 على ما يلي:

"يعاقب بالحبس من ثلاث أشهر إلى سنتين وبالغرامة من مليون الى عشرين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين كل من أقدم، بنية الغش، على الوصول أو الولوج الى نظام معلوماتي بكامله أو في جزء منه أو على المكوث فيه.
تشدد العقوبة الى الحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مليونين إلى أربعين مليون ليرة، إذا نتج عن العمل إلغاء البيانات الرقمية أو البرامج المعلوماتية أو نسخها أو تعديلها أو المساس بعمل النظام المعلوماتي."

إلخ. إلى سرقة عبر الأجهزة الإلكترونية وبالولوج غير المشروع إليها، وباستغلال طاقة معالجتها للتعدين واستخراج العملات التشفيرية على حساب الغير.

لا شك من ارتفاع نسب التعدين غير المشروع في السنوات الماضية الأخيرة، فيرى العديد من الخبراء ومنهم كيفن هايلي **Kevin Haley** [300] بقيام ترابط بين قيمة العملات التشفيرية والتعدين غير المشروع، فلطالما تتمتع هذه العملات بقيمة معينة لن يتوقف الفاعل من سرقة طاقة الأجهزة للتعدين؛ خصوصاً بأنها وسيلة أسهل من السرقة، فشعار التعدين غير المشروع يكمن بـ "إن لم تستطع من سرقتها (العملة)، قم بتعدينها على حساب غيرك".

[300] Director of Symantec Security Response

الفصل الثاني: التقليد الرقمي

يوازي قِدم عهد فعل التقليد وجود المال بحد ذاته، وإن تطوره عبر الزمن اتّبع تطور المال والنقود[301]. تاريخياً، تُعتبر المملكة الليدية المنشئ الأول للنقود المعدنية الرسمية وذلك في القرن السابع قبل الميلاد في عهد الإمبراطورية اليونانية. تُعتبر من أول أوجه التقليد في التاريخ، تعرّض النقود المعدنية التابعة لهذه الإمبراطورية إلى الغش والتقليد من خلال استصناع نسخ منها عبر مزج أو الاستعاضة عن الذهب والفضة بمعادن أقل قيمة[302].

منذ حينه، تطورت أوجه وسبل التقليد والتزوير بأشواط بالتزامن مع طبيعة النقود والعملات المعتمدة. فمن المعادن إلى النقود الورقية إلى النقود الإلكترونية الرقمية. فهل تتعرض العملات التشفيرية إلى التقليد والتزوير بما معناه التقليدي؟ ومن أي منظار يتناول القانون هذا الأمر.

سنعالج في البداية موضوع إمكانية تقليد وتزوير العملات التشفيرية لننتقل إلى أبرز الوجهات القانونية التي تعالج المسألة المطروحة.

المبحث الأول: الإنفاق المضاعف

إن فعل تقليد وتزوير النقود الورقية أو المعدنية الرسمية جرم معاقب عليه في القوانين الداخلية. وبهدف ارتكاب هذه الأفعال، يُقدم الجاني على استصناع عملة ورقية أو معدنية صادرة عن جهة رسمية، الأمر الذي يمكّنه من "خلق" أموال مزيفة يضاعف بموجبها مقدار الأموال التي كانت بحوزته.

301 Reid Goldsborough. “The Lydian Lion: a case for the world's first coin.” The Journal of the Classical & Medieval Numismatic Society, Series Two, Vol. 5.3, September 2004, pp. 111-125.

302 Mark Cartwright. “Ancient Greek Coinage.” Ancient History Encyclopedia, 15 Jul. 2016, www.ancient.eu/Greek_Coinage/, Accessed 22 Jun. 2019.

في العالم الرقمي، من السهل جداً إعداد عدة نسخ من ملف أو معلومة معينة، فالإمكانية متاحة لمضاعفتها وإعداد نسخ غير محدودة منها. بدورها واجهت العملات الرقمية في نماذجها الأولى من هذه المشكلة وعانت من عواقب هذه الثغرة التي استغلها القراصنة لزيادة أرصدتهم بطريقة مبتكرة كُرِّست بإنفاق العملة عينها لأكثر من مرة، ولقد أُطلق على هذا الفعل تسمية الإنفاق المضاعف **Double-Spending** [303]. وفي طبيعة الحال، يقتصر ميدان فعل الإنفاق المضاعف في العالم الرقمي فقط دون المادي.

تتبلور هذه الثغرة في النظام المالي المركزي، فالمستفيد من العملية كالتاجر على سبيل المثال ليس بمقدوره أن يتحقق من إنفاق المستهلك للعملة بشكل مضاعف، ويتمثل الحل لهذه المسألة باللجوء إلى سلطة مركزية موثوق بها أو جهة أخرى تُقدم على المراقبة والتحقق من عدم تعرّض أي عملية تحويل مالية إلى الإنفاق المضاعف[304]. إن مشكلة هذا النظام المركزي هو اتكاء النظام المالي بأكمله على شركة أو جهة معينة مُحتكِرة تدير وتراقب كافة العمليات، أي التعامل مبني على **عنصر الثقة** الذي بدوره قابل للخرق.

هنا أتت ورقة بيتكوين البيضاء المنشورة في العام 2008 تقترح حلاً لمسألة الإنفاق المضاعف والنظام المبني على الثقة، وذلك عبر شبكة النظير للنظير **Peer to Peer** المعتمدة على أنظمة إثبات العمل **Proof of Work** عبر استخدام خادم ذي طابع زمني موزّع **Distributed Timestamping Service**. وبالنتيجة، استُبدل عنصر الثقة بالدليل المشفّر **Cryptographic Proof** الذي يحمي التاجر الإلكتروني (على سبيل المثال) من التعرض للاحتيال الإلكتروني.

يكمن دور هذه الشبكة اللامركزية أي البلوكشاين بتسجيل وتدوين الطابع الزمني للتحويلات من خلال دمجها في سلسلة مستمرة من انظمة إثبات العمل **Proof of Work system** [305] القائمة على

---

[303] يسمى أيضاً بالـ Race Attack.

[304] كالمصارف أو مثلاً شركة PayPal.

[305] شبيهة لنظام Adam Back المعروفة بـ Hashcash والتي اعتُمدت للحد من رسائل ترويج أو تسويق غير مستدرجة SPAM وهجمات حجب الخدمة Denial of Service Attacks.

الهاش **Hash**، بحيث يكوّن سجل عام غير قابل للتعديل من دون إعادة تشغيل نظام الإثبات بأكمله. إن السلسلة الأطول **Longest Chain** تُعتبر اثباتاً لتاريخ الأحداث والمعاملات، وإن بروتوكول الإجماع **Consensus Protocol** في هذا النظام يفترض أن أطول سلسلة مقترحة من قبل الشبكة، يتم قبولها على أنها السجل العام الصحيح الموثوق به والمقبول من المعدنين. تعتبر سلسلة على أنها الأطول إذا كانت نتيجة العمل والجهد الأكبر من قبل المعدنين[306] أو استهلكت الكمية الكبرى من الطاقة من وحدات المعالجة المركزية **CPU Power**.

يشرح "ناكاموتو" بأنه طالما أن الشبكة تُدار من قبل عُقَد/معدنين "صالحين" أو "نزيهين"، وأن غالبية قوة المعالجة بيد هؤلاء الذين يعملون جاهداً لتكوين السلسلة الأطول، فتكون الشبكة بأمان من الذين يتآمرون لمهاجمتها.

- **هجمة 51% على شبكة البلوكشاين:**

كما تبيّن، تعتمد شبكة البلوكشاين وبحسب تفسير ورقة البيتكوين البيضاء على المشاركين "النزيهين" في الشبكة، الذين يسيطرون على 51 بالمئة من طاقة وحدة المعالجة المركزية لمعالجة الكتل التي تحتوي على أحدث البيانات التي سيتم قبولها في السجل العام. يتعاون المشاركين أو العُقَد النزيهين معاً لتأكيد الترتيب الزمني لجميع المعاملات على الشبكة بهدف التحقق من صحة العملية/الصفقة ليتم تبعاً إما قبولها أو رفضها. عند القيام بذلك، تقوم الشبكة بإنشاء سجل غير قابل للتعديل يحتوي على جميع المعاملات والأرصدة وتعتبر السلسلة الأطول على أنها النسخة الصحيحة والموثوق بها للسجل العام.

ولكن، ماذا يحصل إذا ما طرأ تغيير على هذه الآلية؟

[306] Jonathan Chiu, and Thorsten V. Koeppl. Paper on **Incentive compatibility on the blockchain**, Bank of Canada, No. 2018-34, July 2018, https://www.bankofcanada.ca

في ورقة البيتكوين البيضاء، اشترط ساتوشي ناكاموتو وبهدف المحافظة على أمن النظام بأن تتحكم أكثرية العُقد النزيهة بطاقة وحدة المعالجة المركزية. فإذا ما وُجدت مجموعة أخرى من العُقَد المتعاونة سيئة النية، واستطاعت من التحكم بأكثرية طاقة وحدة المعالجة المركزية، تكتسب هذه الأخيرة سلطة إعادة كتابة تاريخ المعاملات السابقة وبالتالي إمكانية إنشاء سلسلة أطول أخرى تمكّنهم من تعديل تاريخ التحويلات والمعاملات، توصلاً الى استعادة العملة التشفيرية التي تم إنفاقها. إنّ هذه العملية تسمى بهجمة الـ 51% وهي التي تمكّن من تحقيق الإنفاق المضاعف.

إنّ شبكات البلوكشاين الصغيرة أو الخاصة هي العرضة لهجمة الـ 51%. لقد ثبت قيام ترابط وثيق بين نسبة تعرض شبكة معينة إلى الهجمة وبين حجم هذه الشبكة، فكلما كبرت الشبكة تقلّصت نسبة تعرضها لهجمة ناجحة[307]. لا مندوحة بأن هذه الهجمة قلما تُشنّ بحيث سُجلت بضع هجمات على مدار السنين، وإنّ شبكات البلوكشاين التابعة للعملات البديلة **Altcoins** هي التي تعرّضت إلى هذه الهجمة. ففي شهر أيار من العام 2018، استُهدفت شبكة البيتكوين الغولد **Bitcoin Gold**، بحيث نجح مخترق الشبكة بإحداث أضرار بقيمة 18 مليون دولار أميركي عبر إرساله لعدد معين من عملة بيتكوين غولد إلى منصة تداول واستبدال عملاته بعملات تشفيرية أخرى، وأقدم لاحقاً على استرجاع العملات التي قام باستبدالها في بداية الهجمة[308].

تتمتع شبكات البلوكشاين الكبيرة كتلك البيتكوين، بالحصانة والمناعة بوجه هذه الهجمة. وهذا ما أثبتته دراسات عديدة منها لمصرف كندا[309]، بحيث أقامت الدليل على أن ارتكاب الإنفاق المضاعف على

---

307 Cyber Threat Alliance. Report on **The Illicit Cryptocurrency Mining Threat**, Op.cit., p. 23.

308 Osato Avan-Nomayo. "51 Percent: Hackers Steal $18 Million In Bitcoin Gold (BTG) Tokens." Bitcoinist.com, 26 May 2018, https://bitcoinist.com/51-percent-attack-hackers-steals-18-million-bitcoin-gold-btg-tokens/, Accessed 2 Dec. 2018.

309 Chiu, and V. Koeppl. **Paper on Incentive compatibility on the blockchain**. Loc.cit.

شبكات البلوكشاين الكبيرة "غير واقعية" وغير ممكنة، ولقد لقي هذا الرأي تأييد العديد من التقنيين والمختصين[310].

وعلى كل الأحوال، كلفة محاولة إنجاح هكذا هجمة على هذه الشبكات تكون عالية جداً، مما يقلّص نسبة الأرباح المرتقبة من المخترقين. فبتاريخ إعدادنا لهذه الرسالة، قدّر موقع **app.crypto51.** تكلفة ساعة واحدة من هجمة 51% يستهدف شبكة البيتكوين بـ $1,021,768 [311]، مع العلم بأن ساعة واحدة لن تكون كافية لإنجاز المهمة. وقد قدّر البعض أن طاقة الكهرباء المطلوبة في الحالة المذكورة توازي الطاقة التي تغذي بلاد مثل مملكة المغرب العربي[312]... فلا شك بأن التكلفة المرتفعة والطاقة الهائلة تشكلان حائلاً وعاملاً غير محفّز أمام المجرم السيبراني.

لا شك بأن البلوكشاين وُجد ليحلّ ثغرة الإنفاق المضاعف التي كانت تعاني منها بعض العملات الرقمية[313]. فكما رأينا إن الشبكات الكبيرة وبالأخص شبكة البيتكوين من المستحيل إنجاح عملية إنفاق مضاعف عليها إذا ما تم احترام نظام التشغيل[314]. وكما بيّنا مسبقاً بأنه يمكن الإنفاق المضاعف عبر

---

[310] Marco Cavicchioli. “What Is and How Double-Spending Works? - NovaMining Media.” Medium, *NovaMining Media*, 4 Jul. 2018, medium.com/novamining/what-is-and-how-double-spending-works-ee45e6433910, Accessed 29 Sept. 2018.

[311] https://www.crypto51.app/

[312] Mitchell Moos. “Analysis: Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco.” CryptoSlate, 29 Nov. 2018, cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/, Accessed 17 Jan. 2019.

[313] Team InnerQuest Online. “How Does a Blockchain Prevent Double-Spending of Bitcoins?” Medium, *InnerQuest Online*, 25 Aug. 2018, medium.com/innerquest-online/how-does-a-blockchain-prevent-double-spending-of-bitcoins-fa0ecf9849f7, Accessed 11 Jun. 2019

[314] Cavicchioli, Marco. “What Is and How Double-Spending Works? - NovaMining Media.” Loc.cit.

هجمة الـ 51% والتي بدورها شبه مستحيلة الإنجاح؛ فباتساع الشبكات على مدار الساعة، تزداد نسبة هذه الاستحالة[315].

كل هذا يجعلنا نتساءل عن دور المشرّع اللبناني من التقليد والتزوير الرقمي... وهذا ما سنبحثه في المبحث الثاني.

المبحث الثاني: التقليد الرقمي في القانون اللبناني

النقد الإلزامي أو الرسمي **Fiat Currency** عبارة عن وسيلة تبادل وتعامل مالي، تتمتع بقيمة معينة وتصدر بإذن الدولة وكنتيجة لها غطاء قانوني **Legal Tender**. تعتبر النقود الرسمية إحدى أوجه سيادة الدول ولكي تكتسب هذه الدول ثقة المواطنين وتدفعهم للتعامل بعملتهم ونقودهم الرسمية باطمئنان، عليها تأمين أقصى درجات الحماية لهذه النقود سواء من الجهة الاقتصادية والمالية أو من الجهة القانونية. لذلك، جرّمت السلطات التشريعية الأفعال التي تمس بصحة وقيمة النقود الرسمية، من هذه الأفعال نذكر التقليد والتزوير والتزييف والإصدار والترويج...

بدوره، جرّم المشترع اللبناني هذه الأفعال عبر المواد 440 حتى 449 من قانون العقوبات اللبناني، وذلك ضمن النبذة الثانية من الفصل الأول من الباب الخامس الخاص بالجرائم المخلة بالثقة العامة. إن موضوع هذه الجرائم القصدية هي العملات المعدنية من ذهبية وفضية أو غيرها والنقود الورقية، ولكن اشترط المشترع اللبناني بأن تكون هذه العملات أو النقود متداولة شرعاً أو عرفاً في لبنان أو خارجه. ولقد

---

[315] مع العلم بأن الدراسات الأولية التي تعود إلى فترات نشأت البيتكوين، تدل على امكانية حصول الإنفاق المضاعف على الشبكة، إلا أن هذا الرأي قد تم دحضه بعد الاتساع الهائل للشبكة في السنوات الأخيرة.

-Mauro Conti, et al. "A Survey on Security and Privacy Issues of Bitcoin." IEEE Communications Surveys & Tutorials, Vol. 20.4, 2018, pp. 3416-3452.

اشترطت المادة 443 [316] من قانون العقوبات بشكل خاص بأن تكون النقود الورقية مصرفية لبنانية أو أجنبية صادرة بأذن الدولة، مما يعني أوراق النقد الصادرة عن المصارف المركزية بناء على تفويض قانوني من الدولة التي تعطيها قوة التداول القانوني[317].

أما لجهة أوجه ارتكاب هذه الجرائم، فلقد عرّف البعض فعل تقليد العملة على أنه "صناعة عملة على مثال العملة الصحيحة، فهو اصطناع عملة مزيّفة تقليداً لعملة صحيحة، أي مشابهة لها في شكلها ووزنها وحجمها، كصناعة قطعة معدنية تحمل النقوش والعبارات والرسوم ذاتها التي تحملها القطع النقدية الصحيحة الرسمية المتداولة، أو طباعتها على أوراق مماثلة لما تحمله العملة الورقية الصحيحة..."[318].

بدوره، فرّق الاجتهاد اللبناني[319] بين فعلي التقليد والتزوير، معتبراً بأن التقليد يقوم على صنع أو اصطناع عملة معدنية أو ورقية، وبأن التزييف أو التزوير هو اجراء تحريف وتحوير للعملة المعدنية أو الورقية الصحيحة في الأصل بطريقة تؤدي الى منح هذه العملة قيمة مختلفة عن قيمتها الحقيقية، وإن هذا التفريق بين فعلي التقليد والتزييف أو التزوير لا يقتصر على ما تنص عليه المادتين 441 و442 من قانون العقوبات بشأن العملة المعدنية، بل يتم اعتماده فيما يتعلق بالعملة الورقية بحسب المادتين 443 و444 عقوبات.

---

316 تنص المادة 443 من قانون العقوبات اللبناني على ما يلي:

"من قلد أوراق النقد أو اوراق النقد المصرفية اللبنانية أو الأجنبية الصادرة بأذن الدولة بقصد ترويجها أو اشترك بإصدارها أو بترويجها عوقب بالعقوبات المنصوص عليها في المادة الـ 440."

317 سمير عالية وهيثم عالية، **القانون الجزائي للأعمال**، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الاولى، 2012، ص. 249.

318 نادر عبد العزيز شافي، " جرائم التزييف والتقليد والترويج النقدي"، مجلة الجيش، العدد 285، آذار 2009، https://www.lebarmy.gov.lb/ar/content/285-m%20.

319 محكمة التمييز الجزائية الغرفة السادسة، الرئيس رالف رياشي والأعضاء /عالية//سماحة/، قرار رقم 202 تاريخ 1997/12/23، منشور على موقع الجامعة اللبنانية مركز الأبحاث والدراسات في المعلوماتية القانونية، www.legiliban.ul.edu.lb

هذا بإيجاز ما نص عليه قانون العقوبات اللبناني لجهة تقليد العملات الرسمية... ولكن مؤخراً استحدث المشترع وجهاً حديثاً لفعل التقليد وذلك بموجب قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، فمن الجدير التطرق إلى ما ورد فيه لهذه الجهة.

- **جرم تقليد النقود الإلكترونية أو الرقمية بموجب القانون 2018/81:**

جرّم المشترع اللبناني بموجب الفقرتين 4 و5 من المادة 116 من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي فعل تقليد "النقود الإلكترونية أو الرقمية" وفعل استعمال هذه النقود مع العلم بطبيعتها، وأضفى الوصف الجنحي على هذين الفعلين عبر فرض عقوبة الحبس و أو الغرامة المالية[320].

غير أن هذه المادة تثير اشكاليتين، الأولى على الصعيد التقني والثانية على الصعيد القانوني. تقنياً، تكمن الإشكالية باستعمال المشرّع عبارة "قلّد" بل بالأحرى تجريم فعل تقليد "النقود الإلكترونية أو الرقمية"[321]، فالعملات التشفيرية عبارة عن رموز وبيانات رقمية تشفيرية تعتمد على تقنية البلوكشاين والتي يتعذّر التلاعب بها نظراً لآلية عملها، مما يجعل عملية تقليد أو تزوير عملة تشفيرية بكيانها الإلكتروني

---

[320] تنص المادة 116 من القانون رقم 2018/81 على ما يلي:

"يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبالغرامة من عشرة ملايين إلى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من:

1- قلد بطاقة مصرفية او زورها.

2- استعمل أو تداول، مع علمه بالأمر، بطاقة مصرفية مزورة او مقلدة.

3- قبل قبض مبالغ من النقود مع علمه بأن الايفاء تم بواسطة بطاقة مصرفية مزورة او مقلدة.

4- قلد نقوداً الكترونية أو رقمية.

5- استعمل، مع علمه بالأمر، نقوداً الكترونية او رقمية مقلدة.

6- قلد شيكاً الكترونياً أو رقمياً.

7- استعمل مع علمه بالأمر، شيكاً الكترونياً أو رقمياً مقلداً.

تطبق أحكام المادتين 114 و115 على الأفعال الجرمية المذكورة في هذه المادة."

[321] ماريلين أورديكيان، "العملات الافتراضية المشفّرة في الحقل الجنائي السيبراني"، مجلة الدفاع الوطني، العدد 108، نيسان 2019، الصفحات 73-105، ص. 95، https://www.lebarmy.gov.lb/ar/content/108-d

بالأمر المستحيل تقنياً، وإن التوجّه السائد من الفقه يقرّ بوجود هكذا استحالة[322]. فشبكة البلوكشاين العلنية وبالأحرى العُقد، لن تقبل ولن تصدّق على نموذج مزور أو مقلّد من عملة تشفيرية، هذا **إذا** ما استطاع أحد من تزويرها أو تقليدها من الأساس... حينه جلّما نكون أمام محاولة جرمية وذلك لعدم اكتمال العنصر المادي من الجرم لنكول النتيجة الجرمية، فيعاقب على هذه المحاولة بحسب المادة 115 من القانون 2018/81.

وبالتالي، إن أقرب فعل للتقليد في هذا النطاق هو فعل الإنفاق المضاعف **Double-Spending** الذي عولج في المبحث السابق. وكما تم التبيان مسبقاً، بأن حتى الإنفاق المضاعف يبقى في النطاق النظري عندما نتحدث عن شبكات بلوكشاين عامة وهائلة كتلك البيتكوين بحيث يغدو إنجاح عملية الإنفاق المضاعف في الواقع بالأمر المستحيل، وهذا ما أكدته عدة دراسات منها المجراة من قبل مصرف كندا المركزي[323].

أمام هذا الواقع، يكون المشترع اللبناني قد خلط ومزج بين البطاقات المصرفية والشيكات سواء الورقية أو الإلكترونية التي تقبل التقليد والتزوير، على عكس العملات التشفيرية التي بطبيعتها ولتاريخنا ليس من الممكن تقليدها أو تزويرها.

أما قانونياً وكما بحثنا مسبقاً، لقد اشترط المشترع اللبناني في المواد المجرّمة لأفعال التقليد والتزوير والترويج بأن يكون موضوعها معادن ونقود ورقية متداولة شرعاً أي صادرة عن مصرفٍ مركزي أو جهة

---

322 Jamie Redman. "When It Comes to Scarcity and Anti-Counterfeiting Bitcoin Actually Outshines Gold." Bitcoin News, 11 Apr. 2017, news.bitcoin.com/scarcity-anti-counterfeiting-bitcoin-outshines-gold/, Accessed 27 Nov. 2018.

-أيضاً:

-James J. Angel, and Douglas McCabe. "The ethics of payments: Paper, plastic, or bitcoin?" Journal of Business Ethics, Vol. 132.3, 2015, pp. 603-611, p. 606.

323 Max Yakubowski. "Bank of Canada Study Finds Double Spending in Blockchain is 'Unrealistic'." CoinTeleghraph, 22 Jul. 2018, https://cointelegraph.com/news/bank-of-canada-study-finds-double-spending-in-blockchain-is-unrealistic, Accessed 2 Dec. 2018.

رسمية أخرى. مما يعني أن النقود الصادرة عن جهة رسمية كالمصرف المركزي أو المتعامل بها عرفاً في لبنان هي فقط بحمى قانون العقوبات اللبناني، وكل عملة أو وسيلة دفع لا تستحصل على هذا الشرط تقع خارج نطاق الغطاء القانوني.

إن المادة 116 من القانون رقم 2018/81 أتت وجرّمت فعل تقليد "النقود الإلكترونية أو الرقمية" وفعل استعمالها مع العلم بحقيقتها، بالرغم من عدم تمتع العملات التشفيرية وسائر أنواع العملات الرقمية بالصفة الرسمية في لبنان ومع العلم بأنها لا تصدر عن جهة رسمية كالمصرف المركزي[324] ولا يتم التعامل بها عرفاً. وبما أن النص القانوني الجديد يعدّل ويحل مكان النص القديم (في المبدأ)، وهذه قاعدة قانونية أساسية، فهل نعتبر بأن المشترع اللبناني قد عدّل عبر المادة 116 مواد قانون العقوبات وألغى اشتراط الصفة الرسمية ومشروعية العملات؟ بمعنى آخر، هل ألغى المشترع شرط مشروعية العملة موضوع جرائم التقليد والتزوير؟ أم أن الصياغة تمت من دون الانتباه إلى هذا الأمر؟

[324] تُستثنى هنا العملات الرقمية التي تعمد بعض المصارف المركزية حاليا إلى اصدارها، فهذه العملات تعتبر رسمية وتكون متساوية لجهة الحماية القانونية مثلها مثل النقود المادية الرسمية.

الخاتمة

عرضنا في دراستنا التنظيم التقني والقانوني لعملة البيتكوين والعملات التشفيرية ومدى انخراطها وتأثيرها في عالم الجريمة. ونظراً لحداثة الموضوع، كان لا محال أن تستهل الدراسة بتفريق أنواع العملات الرقمية واستعراض المصطلحات العديدة التي تُطلق عليها، وذلك لأن تعدد هذه المصطلحات والعناوين تعتبر أول مشكلة تُعيق تكريس حل تشريعي وتنظيمي. وإن توحيد المصطلحات يغدو بداية حل الفراغ و أو الاختلاف في التشريع، الأمر البالغ في الأهمية نظراً لطبيعة هذه العملات العالمية والعابرة للحدود التي تكسر القيود والتجارب المحلية لتقييدها. من هنا، كان لا بدّ من استعراض أهم سمات وخصائص العملات التشفيرية مع أخذ عملة البيتكوين (التي تعتبر العملة التشفيرية الأم) نموذجاً، نظراً لأن هذه الخصائص الحديثة هي التي جعلت منها ابتكاراً لا مثيل له في عالم التكنولوجيا، وهي التي تؤثر مباشرةً على آلية تفاعل القوانين مع مفاعيلها.

لاشكّ بأم العملات التشفيرية تخطّت العالم الرقمي، فلم تعد عملة افتراضية غير ملموسة مثلها مثل سائر أنواع العملات الرقمية والافتراضية، بل ارتدّت وأضحى لها تمثيل رقمي مالي في العالم الواقعي، لذلك توصلنا بادئ ذي البدئ بأنه من الخطأ وضعها في خانة العملات الافتراضية الرقمية، فهي عملات مستقلة عن سوابقها ولها ترابط مباشر مع العالم الاقتصادي والنقدي. لذلك كان من الضروري البحث بأهم المميزات التي تتجلى بها ومنها خاصية اللامركزية التي حررت العملة من قيود السلطة المركزية والجهات الثالثة الوسيطة، بحيث تم استرداد الحرية في التعامل النقدي. فرأينا بأن وجود طرف ثالث إضافي في التحويلات هو مصدر خطر بحد ذاته، لأنه يحمل احتمالات للفشل الأمني والتقني، على عكس نظام العملات التشفيرية العصية على الهجمات السيبرانية. وأن التعامل عبر الوسيط يجعل العملاء عُرضة للمراقبة، لا بل تكون بيانات هؤلاء الشخصية تحت تصرف هذا الوسيط الذي كثيراً ما يُسيء استخدامها أو يفشل بحمايتها عند المواجهة مع جهات ثالثة خارجية، ولذلك تكمن أهمية نظام العملات التشفيرية الذي يُثيب الخصوصية الرقمية للعملاء عبر تفادي التصريح عن البيانات الشخصية وعبر إقصاء الحاجة للثقة بطرف ثالث المركزي.

على الرغم من حسناتها، تبلورت مخاطر ذات الأوجه الجمّ خصوصاً لدى ارتفاع قيمتها. من هذه المخاطر تطرقنا إلى الاقتصادية والمالية (مثل اجتياحها الدول ذات الاقتصاد المنهار) وتلك التقنية الأمنية قبل التطرق إلى تلك القانونية، **نظراً لقيام علاقة وثيقة ووطيدة فيما بينها.**

إن المخاطر العديدة وازدياد الإقبال على عملات لا تصدر عن جهة رسمية ولا تدخل ضمن أطر قانوني أثار العديد من المشاكل القانونية، فكيف يمكن التعامل بعملة ليست بالرسمية؟ كيف يمكن القبول بعملة رقمية كوسيلة دفع وتبادل وهي صادرة عن جهة مجهولة أو تابعة للقطاع الخاص؟ وهل هي نقود في بادئ ذي الأمر؟ نتيجةً لتعاظم المساوِئ، سرعان ما استدرك المشرع ضرورة إحاطة العملات التشفيرية بالأطر القانونية، فاختلف نهج كل دولة بحيث تبلورت ثلاث مواقف قانونية: 1) نهج الحظر والمنع التام 2) التقبّل والتشريع والاحتضان 3) التريّث والاكتفاء بالتحذير والتوجيه **Wait and See Approach.** في حين يسود الموقف الثالث لدى أكثرية الدول، تبلور في النهج الثاني مواقف متعددة، فالبعض وضع تنظيماً خاصاً بها والبعض اختار شمل العملات بقوانين الريبة والبعض انتقى شملها بقوانين حماية المستهلك، وآخرين في قانون النقد وقانون الضريبة إلخ. في حين انتهز البعض القوانين الراهنة واعتمد التكييف والتفسير الواسع.

أما فيما يتعلق بالموقف اللبناني، فكان لبنان من أول البلدان في المنطقة التي اتخذت موقفاً عبر اتباع المصرف المركزي النهج الثالث المتمثل بإصدار التعاميم والتحذير، فارضاً المنع الجزئي بالتداول فقط على المؤسسات المالية، **مع العلم أن المنع التام لا يجدي لأن هناك دائماً سبل بديلة للتعامل.** ولكن مع ذلك، رحّب مصرف لبنان بفكرة العملات الرقمية بحيث صرّح حاكمه مراراً بأنه يزمع لإصدار عملة رقمية لبنانية، فيبقى السؤال إذا ما كان السوق اللبناني جاهزاً لهكذا خطوة في ظل الأوضاع الاقتصادية المتدهورة... والإشكالية الكبرى تكمن بمدى جهوزية القوانين اللبنانية من مجاراة هذه العملة، في ظل عدم الاعتراف بتمتع المال الرقمي بقيمة مماثلة للمال المادي، فيتبلور هذا النقص على صعيد قانون العقوبات وقانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي الذي لا يعالج الجرائم الإلكترونية الأحدث عهداً ولا يواكب التكنولوجيا الحديثة وبالتالي لا يجدي بالنفع، علماً أن عدداً من ثغرات هذا القانون يجعل بعضاً من نصوصه غير قابلة للتطبيق.

دولياً وإقليمياً، جسّدت الوثائق الصادرة عن مجموعة العمل المالي **FATF** والتوجيه الأوروبي الخامس لمكافحة تبييض الأموال **AMLD5** أبرز الوثائق لتاريخنا التي تُعنى بتنظيم العملات التشفيرية من نواحٍ متباينة. وبالرغم من أن هذه الجهات تعمل جاهدة لإحاطتها بالغطاء التشريعي، إلا أننا استنتجنا بأن محاولاتها تقيّد كثيراً من طبيعة نظام العملات التشفيرية وتسلب الحرية الفردية والخصوصية النقدية، فكل القيود التي وضعتها ولا تزال تضعها تحاول من أقلمة العملات التشفيرية إلى الأنظمة المالية الراهنة التقليدية **في حين أن هذه العملات لها سياسة نقدية حديثة مستقلة تتطلب نظاماً مستقلاً خاصاً بها.**

في المقابل، وبعد فهم آلية عمل العملات التشفيرية ومدى قانونيتها ومخاطرها، انتقلنا إلى القسم الخاص وعالم الجريمة بحيث وكالمعتاد كان المجرم سبّاقاً من إيجاد ما يستغله لمنافعه الجرمية ماكثاً بعيداً عن متناول سلطات إنفاذ القانون والقضاء. فولدت طرقاً حديثة لارتكاب الجرائم التقليدية، لا بل تبلورت أفعال غير مشروعة جديدة بطبيعتها وغير قابلة للتكييف مع النصوص الراهنة. ولم يكتفِ المجرم باقتراف جرائم العملات التشفيرية على حدة، بل عمد في الكثير من الأوقات إلى دمجها مع حقول وتقنيات أخرى أبرزها شبكة الإنترنت المظلمة وأجهزة إنترنت الأشياء والبيانات الشخصية الرقمية. فهذه التقنيات والبيانات التي غدت الرأسمال الرئيسي في عالم التجارة والاقتصاد الإلكتروني، أضحت أداةً جرمية تسهّل ارتكاب جرائم العملات التشفيرية.

وبالتالي، بعد أن عرضنا أبرز الجرائم التي تُرتكب بواسطتها أو تتعرض لها توصلاً إلى الجواب لإشكالية مدى اعتبار أو تكوين العملات التشفيرية لعملة بيد المجرمين. عرضنا مواقف قانونية دولية وإقليمية وداخلية والتنظيم القانوني، فتبين لنا أن لا توحيد دولي حيال الجرائم والأفعال غير المشروعة هذه. وإن أكثرية القانونيين في ظل معارضة التقنيين، يعتقدون بأن هذه العملات هي عملات المجرمين.

برأينا إن هذه العملات ليست بعملات المجرمين، وإن الجرائم والأفعال غير المشروعة التي بحثنا فيها هي جرائم تنتمي إلى فئات متنوعة ولكن تُقترف في السيناريو التقليدي اليومي بواسطة النقد الرسمي، لا بل وتيرة ارتكابها عبر هذه الأخيرة تضاهي أضعاف ارتكابها بالعملات التشفيرية وإن هذا الأمر لا يجعل منها عملةً للمجرمين، فهي ليست إلا وسيلة بأياديهم مثلها مثل أي أداة أخرى تصلح لارتكاب الجرائم، ونحن نرفض رفضاً تاماً اعتبارها عملةً لهؤلاء أو أداةً جرمية بطبيعتها وبحد ذاتها.. لقد دعمنا رأينا هذا عبر عرض خصائص تقنية البلوكشاين وبيّنا بأن كافة التحويلات يتم تسجيلها على السجل العام العلني مما يسمح بتتبع العمليات والتحويلات، فكل ما نحتاجه هو تطوّر وجهد إضافي من قبل سلطات الملاحقة وإنفاذ القانون لفهم هذه التقنية والاستفادة منها بدلاً من تجاهلها.

وبناء على ما تقدم، نقترح التالي:

– إن ميل الأفراد والمنظمات الإجرامية والإرهابية وبعض الدول إلى استخدام العملات التشفيرية لتفادي القوانين المحلية والدولية، يتطلّب اتخاذ إجراءات من جانب كافة الدول. فمن الحكمة بادئ ذي البدء أن تقوم كل دولة بمفردها على تطوير نهجها التشريعي الخاص الذي يجمع ويشمل بين التنظيم والتبني والتحذير من جوانب معينة. على أن يتم تبني معاهدات وصكوك على الصعيد الدولي تعالج مسألة الصلاحية القضائية، وتعزز التعاون بملاحقة المجرمين وتعالج مسألة تسليم هؤلاء وما تم مصادرته.

– تبني سياسة خاصة بالعملات التشفيرية واعتبارها فئة مستقلة من الأموال بموجب قانون مستقل، وتفادي دمجها أو اعتبارها من إحدى فئات الأموال الراهنة وذلك نظراً لطبيعتها المميزة والفريدة.

– للتغلب على لامركزية العملات التشفيرية، على المشرعين استهداف منصات التحويل والوسطاء الذين يعتبرون سلطة مركزية يمكن استهدافها بالتنظيم والتشريع المباشر.

– قد يشكّل نظام العملات التشفيرية غير المنظم خطراً على فعالية القوانين الراهنة، وبالتالي على المشترع ضمان عدم تقويض هذه العملات للأنظمة والقوانين الراهنة. لذلك، يجب إدخالها فوراً ضمن هذه الأنظمة والقوانين كقانون العقوبات وقانون حماية المستهلك مثلاً تفادياً للفراغ التشريعي أو التفسير الواسع.

– إجراء تقييم للمخاطر وتعزيز الوعي بها وبالإيجابيات المتعلقة باستحواذ واستخدام وتداول هذه العملات، وفرض رقابة على شبكة الإنترنت المظلمة، واستغلال النتائج المستخلصة من هذه التقييمات لوضع استراتيجيات للنهج التنظيمي ونهج لإنفاذ القانون على المدى القصير والمتوسط والطويل.

– إن المجرم دائماً على مقدمة من سلطات الملاحقة وأسرع تكييفاً للتقنيات الحديثة، وكنتيجة يجب على الدول تسريع الجهود لتطوير المعرفة والاستثمار بالموارد البشرية والتقنية واستحداث برامج تدريب استراتيجية لجميع الموظفين المختصين في إنفاذ القانون، كما يجب عليها تطوير فهم تقني أساسي عملي لدى سلطات الملاحقة لدعم استمرارية العمليات.

– تمكين الشراكة بين القطاعين العام والخاص. فلا يمكن للقطاع العام تطوير تنظيم فعال وتعزيز المعرفة وتحسين الاستخبارات بالعمل بمفرده.

وفي لبنان بشكل أخص، نقترح التالي:

– لبنان ليس بمرحلة من الجهوزية على صعيد البنى التحتية والاقتصاد والقانون لتقبّل هذه العملات وتوابعها، ولكن بغض النظر عن التوجه القانوني الذي سيتخذ يجب المبادرة فوراً إلى الاهتمام بهذه الظاهرة. فمن الضروري جداً (وقبل وضع قانون للجرائم الإلكترونية الأحدث عهداً والذي سيستغرق وقتاً طويلاً) **الاعتراف بالبيانات المعلوماتية والعملات الرقمية (بشكل مستقل عن الدعامة) كمال ذات قيمة أي اعتبارها مال معنوي تساوي المال المادي،** فهذا الأمر يمكّن القضاء اللبناني من تكييف نصوصه الراهنة خصيصاً قانون العقوبات اللبناني على الأفعال التي ترتكب وتكون من صلاحيته النظر بها، وذلك كبداية لتفادي عائق مبدأ شرعية الجريمة والعقوبة. علماً أنه يبقى وضع قانون عقوبات جديد يجاري العصر هو الحل الأنسب، نظراً لأن القانون الراهن أصبح مستنزفاً وقديم العهد ولا يتصف بنصوص ذات الطابع الاستباقي والوقائي.

– بالنسبة إلى ثغرات قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي التي ناقشناها، فيجب كبداية تعديل المادة الأولى منه ليتضمن مصطلحين مستقلين الأول يعرّف النقود الإلكترونية والثاني يعرّف العملات الرقمية والتشفيرية، وذلك تفادياً للدمج والخلط فيما بينهما وتمهيداً لإمكانية تطبيق القانون عليهما، علماً أن غموض النص لا سمح بمعرفة قصد المشرّع الحقيقية من وراء استعماله مصطلح "النقود الإلكترونية والرقمية".

– وتبعاً لذلك، يقتضي تعديل المادتين 61 و64 من القانون المذكور وفقاً للمصطلحات الجديدة ونطاق تطبيقهما تبعاً للآليات المحددة.

– على غرار تعديل المادة 116 (التي عدّلت قانون العقوبات اللبناني) التي تجرّم فعل تقليد النقود الإلكترونية أو الرقمية، علماً أننا بيّنا غموض وسوء استعمال كلمة "التقليد" في ظل عدم إمكانية تقليد العملات التشفيرية.

– تعديل قانون الأصول المحاكمات الجزائية أو الفصل السابع من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي (يتناول القواعد الإجرائية المتعلقة بضبط الأدلة المعلوماتية وحفظها)، لتُمنح الضابطة العدلية والقضاء المختص مهل أقصر والصلاحية بالتحقيق واتخاذ الإجراءات اللازمة مباشرةً عند تلقي شكاوى تتعلق بأفعال تستوجب طابع السرعة، مثل طلب الفدية الإلكترونية ذات المهلة القصيرة.

رأينا أن كثر يحاولون في العالم اليوم البحث عن الوسائل المناسبة لتنظيم العملات التشفيرية قانوناً. باعتقادنا يغدو نهج "صندوق الرمل" الحل الأنسب (لأنه يجنّب تقييد إمكانات التقنية المستحدثة) خصوصاً على صعيد البلدان المنفتحة على التقنيات والتكنولوجيا الحديثة، وذلك كخطوة تمهيدية لتقبّلها. فما شهده العالم بعد هذه الثورة المالية والرقمية ليس كما قبلها، فإذا لم تنجح العملات التشفيرية فمن الأكيد أن نظاماً جديداً وعملةً جديدة ستتبلور وتستبدل النظام النقدي الراهن. ولكن في الوقت الحالي، إن مجرد وجودها يشكّل تهديداً للدول وللمصارف وتذكيراً لها بأن هنالك البديل لإجراء عمليات الدفع والتحويل وبأن احتمال سلب سلطة إصدار النقد والتحكم به هي قائمة ومحدقة. وإذا ما لم تجتهد الدول إلى وضع بعض الضوابط على العملات التشفيرية ولم تقم بسن تشريعات ذات الطابع العقابي التي تجذب عنصر الثقة والاطمئنان على غرار سياسة جنائية تتماشى مع هذا التطوّر، فستتبلور الجرائم والأفعال السابق ذكرها أكثر في ظل غياب القيود والعواقب، ولربما سنشهد أيضاً ظهور أفعال بطبيعتها غير مشروعة ومستهجنة ولكن لا نصوص تجريمية بخصوصها، فسيبقى مرتكبيها من دون الملاحقة... وحينئذ **قد** تتحول العملات التشفيرية إلى عملة المجرمين.

Abbreviations الاختصارات

AML	Anti–Money Laundering
AMLD	Anti–Money Laundering Directive
ATM	Automated Teller Machine
BaFin	The Federal Financial Supervisory Authority
BTC	bitcoin
CFTC	U.S. Commodity Futures Trading Commission
CPU	Central Processing Unit
CRA	Canada Revenue Agency
CTF	Combating the Financing of Terrorism
CVC	Convertible Virtual Currency
Crypto	Cryptocurrency
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DVC	Decentralised Virtual Currency
Eth	Ethereum
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FinTech	Financial Technology
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
ibid	ibidem
id	idem
ICO	Initial Coin Offering
CWP	Custodian Wallet Providers
IMF	International Monetary Fund
IP	Internet Protocol

IS	Information Security
IT	Information Technology
JORF	Journal Officiel de la République Française
KYC	Know Your Customer
Loc. cit.	Loco Citato
MSB	Money services business
No.	Number
Op. cit.	Opere Citato
P2P	Peer to Peer
par.	Paragraph
p.	Page
pp.	Pages
SEC	U.S. Securities and Exchange Commission
SHA	Secure Hash Algorithms
UN	United Nations
UNOCT	United Nations Counter-Terrorism Office
VASP	Virtual Currency Service Provider
VCE	Virtual Currency Exchange
VC	Virtual Currency
Vol.	Volume
XMR	Monero
XVG	Verge
ZEC	Zcash

معجم المصطلحات

-أ-

1. اعرف عميلك – **Know Your Customer (KYC):**

أو المعروفة أيضاً بسياسة اعرف زبونك، هي قاعدة تطبقها الشركات والمؤسسات والمصارف تقوم بموجبها من التحقق من هوية عُملائهم وتقيّم مدى ملاءمتهم، على غرار تقدير المخاطر المستقبلية التي قد تنتج عن ارتكاب أفعال غير القانونية تجاه المؤسسة المعنية.

2. الإنترنت العميق – **Dark Web:**

قسم من محتوى شبكة الويب العالمية، غير ظاهرة من قبل محركات البحث السطحية ولا يمكن الوصول إليها إلا باستخدام برامج معينة أو تراخيص محددة.

3. الإنفاق المضاعف – **Double-spending:**

إنفاق العملة الرقمية عينها لمرتين.

-ت-

4. التعدين – **Mining:**

استعمال القوة الحسابية لمعالجة العمليات على شبكة البلوكشاين بهدف الحصول على جائزة كمقابل، بحيث يتم إضافة المعاملات المتحقق من صحتها إلى الشبكة وذلك عبر نظام إثبات العمل.

5. تقنية التشفير – **Encryption:** آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن ارجاعها إلى حالتها الأصلية. قوام هذه التقنية هي خوارزمية **Algorithm** رياضية ذكية تسمح لمن يمتلك مفتاحاً سرياً، بأن يحوّل رسالة مقروءة إلى رسالة غير مقروءة والعكس صحيح. أي أنه يتم استخدام المفتاح السري لفك الشيفرة وإعادة الرسالة المشفّرة إلى وضعيتها الأصلية.

-د-

6. دالة هاش التشفيرية – **Cryptographic Hash Function (CHF):**

عبارة عن تابع يقوم بتحويل دخل **Input** معين من الحروف والأرقام إلى مخرج **Output** مشفّر ذات طول ثابت.

-س-

7. ساتوشي – **satoshi:**

أصغر فئة من عملة البيتكوين وتعادل 0.00000001.

8. ساتوشي ناكاموتو – **Satoshi Nakamoto:**

شخص أو جهة مجهولة أقدمت على اختراع نظام البيتكوين.

9. سلسلة الكتل – **Blockchain:**

هي التقنية التي تُبنى عليها العملات التشفيرية. هي عبارة عن سجل عام رقمي تقوم بتسجيل وحفظ كافة العمليات التي تجري عبرها، وليست هناك الإمكانية بالتلاعب بقيودها. تُستخدم التقنية بحد ذاتها في مجالات أخرى، مثل القطاع الصحي والعقود الذكية إلخ.

-ش-

10. شبكة النظير للنظير – **Peer to Peer Network (P2P):**

في هذه الشبكة، يعتبر الـ **Peers** "الأقران" أنظمة حاسوب متصلة ببعضها البعض عبر شبكة الإنترنت. يمكن مشاركة الملفات مباشرة بين الأنظمة على الشبكة دون الحاجة إلى خادم مركزي. بمعنى آخر، يصبح كل جهاز حاسوب على هذه الشبكة خادم ملفات وعميلاً في آن واحد.

-ع-

11. العرض الأولي لعملة – **Initial Coin Offering (ICO):**

وسيلة لجمع الأموال، حيث تطلق شركة تتطلع إلى جمع أموال بهدف إنشاء عملة أو تطبيق أو خدمة جديدة. يمكن للمستثمرين المهتمين شراء العرض الأولي لعملة والحصول على رمز عملة تشفيرية جديدة صادرة عن الشركة. قد يكون لهذا الرمز بعض الفوائد في استخدام المنتج أو الخدمة التي تقدمها الشركة، أو قد يمثل مجرد حصة في الشركة أو المشروع.

12. عقدة – **Node:**

جهاز إلكتروني يساهم على شبكة البلوكشاين بطريقة معينة كمعالجة العمليات والحفاظ على نسخة مستحدثة من البلوكشاين.

13. العملات البديلة – **Altcoins:**

يعني كل العملات التشفيرية ما عدا عملة البيتكوين.

14. العنوان – **Address:**

ان عنوان عملة البيتكوين (على سبيل المثال) يتألف من سلسلة أرقام وأحرف، مثلاً DSrBJdB2AnWaRMgBrv5NSC6n89446DavF1

–ك–

15. الكتلة – **Block:**

مجموعة من العمليات ذات الطابع الزمني، تحمل بصمة الكتلة السابقة. إن الكتل المصدّقة، تُضاف عبر التراضي **Consensus** إلى سلسلة الكتل.

16. كتلة التكوين – **Genesis Block:**

أول كتلة على شبكة البلوكشاين، تم تعدينها من قبل ساتوشي ناكاموتو بتاريخ 3 كانون الأول من العام 2009.

–ل–

17. اللامركزية – **Decentralisation:**

انعدام سلطة أو جهة مركزية، مما يعني أن آلية اتخاذ القرار ليس محتكراً من قبل سلطة واحدة بل موزّع على عدد غير محدد من المستخدمين.

–م–

18. المحفظة – **Wallet:**

برنامج أو جهاز يحفظ عناوين العملات التشفيرية والمفاتيح الخاصة. تتجسد وظيفة المحفظة على حفظ معلومات العميل الخاصة. من هذه المعلومات نذكر: أزواج مفاتيح خاصة/عامة؛ الحسابات التي لها عناوين البيتكوين وأموال من المعاملات المختلفة المرتبطة به؛ المعاملات الخارجة والداخلة إلى المحفظة وإعدادات المستخدم.

19. محفظة ساخنة – **Hot Wallet:**

محفظة مرتبطة بشبكة الإنترنت. بالرغم من سهولة إعدادها واستخدامها، إلا أنها قابلة للقرصنة بسهولة أكثر على عكس المحافظ الباردة.

20. محفظة ورقية – **Paper Wallet:**

المحفظة الورقية عبارة عن مستند ورقي يتضمن المفتاح الخاص والعنوان. إن هذه الوسيلة تمكّن من تخزين العملات التشفيرية خارج نطاق شبكة الإنترنت.

21. المخزن البارد – **Cold Storage:**

وسيلة لحفظ العملات التشفيرية خارج شبكة الإنترنت، حيث تكون أكثر أماناً من الهجمات السيبرانية. تجدر الاشارة إلى أنه من المحبذ تخزين الكميات الكبيرة من العملات التشفيرية في المخازن الباردة.

22. المفتاح الخاص – **Private Key:**

يوقّع المفتاح الخاص على معاملات إنفاق العملات التشفيرية الموجودة في المحفظة. يجب أن يبقى هذا المفتاح سرياً في كل الأحوال، لأنه يعتبر بحد ذاته السلطة التي تخوّل من إنفاق العملات.

–ن–

23. نظام إثبات العمل – **Proof of Work (PoW):**

وسيلة لمعالجة العمليات على شبكة البلوكشاين. تسمح للمعدنين بمعالجة العمليات عبر حل عمليات حسابية لقاء الحصول على مقابل كجائزة في حال حلها أولاً.

24. نهج صندوق الرمل التنظيمي – **Regulatory Sandbox:**

عبارة عن مقاربة تنظيمية تسمح للشركات الخاصة والناشئة من امتحان واختبار الابتكارات، في بيئة مراقبة واستثنائية (إعفاءات خاصة، تمويل، وتسهيلات أخرى). يُجيز هذا النهج من مواكبة عصر التطور التكنولوجي السريع خصوصاً في الأسواق المالية (وظهور التكنولوجيا المالية المعروفة بـ FinTech أي Financial Technology)، بحيث يتم اختبار التقنيات الجديدة والخدمات مالية والأطر الحديثة للأعمال، وذلك كمحاولة لمعالجة المعضلة بين رغبة القطاع الخاص في الابتكار ومحاولة المشرع بوضع إطار تنظيمي من دون حد الإبداع التقني.

–هـ–

25. هجمة حجب الخدمة الموزع – **Distributed Denial of Service Attack (DDos):**

جوم سيبراني يسعى فيه مرتكب الجريمة إلى جعل جهاز أو مورد شبكة غير متاح، مما يعطل خدمات تابعة لمضيف متصل بشبكة الإنترنت، وذلك عن طريق الإثقال الزائد للنظام بالطلبات بهدف منع تقديم الطلبات المشروعة.

–و–

26. ورقة بيضاء – **White Paper:**

وثيقة لعرض التفاصيل التقنية لمشروع جديد، تفاصيل مثل آلية العمل والفريق وراء المشروع وخريطة الطريق.

الملاحق

ملحق رقم 1: ورقة البيتكوين البيضاء

Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto

satoshin@gmx.com
www.bitcoin.org

Abstract
A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without re doing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction
Commerce on the Internet has come to rely almost exclusively on financial institutions serving aa trusted third parties to process electronic payments. While the system works well enough formost transactions, it still suffers from the inherent weaknesses of the trust based model.Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting theminimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants mustbe wary of their customers, hassling them for more information than they would otherwise need.A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.
What is needed is an electronic payment system based on cryptographic proof instead of trust,allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily

be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next ownerand adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced **[1]**, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

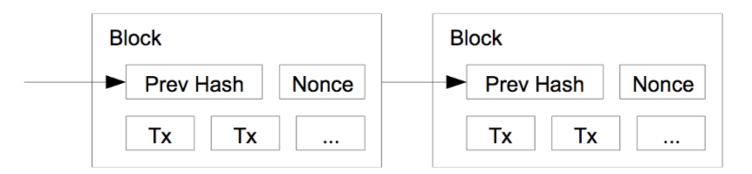
3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at thetime, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hash cash **[6]**, rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits.

Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort investedin it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow thefastest and outpace any competing chains. To modify a past block, an attacker would have toredo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time,the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.

2) Each node collects new transactions into a block.

3) Each node works on finding a difficult proof-of-work for its block.

4) When a node finds a proof-of-work, it broadcasts the block to all nodes.

5) Nodes accept the block only if all transactions in it are valid and not already spent.

6) Nodes express their acceptance of the block by working on creating the next block in thechain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously,

some nodes may receive one or the other first. In that case, they work on the first one they
received,but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

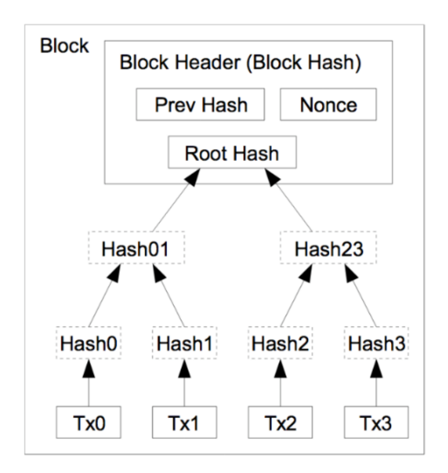
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

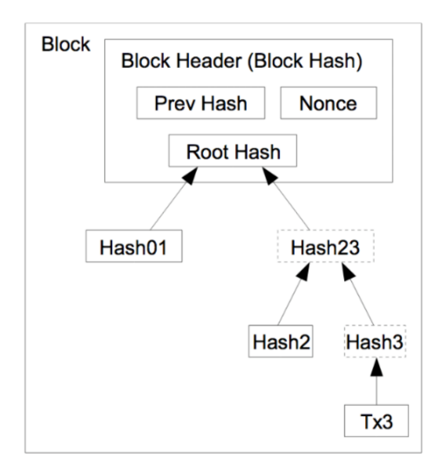
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash,transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash.Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Transactions Hashed in a Merkle Tree

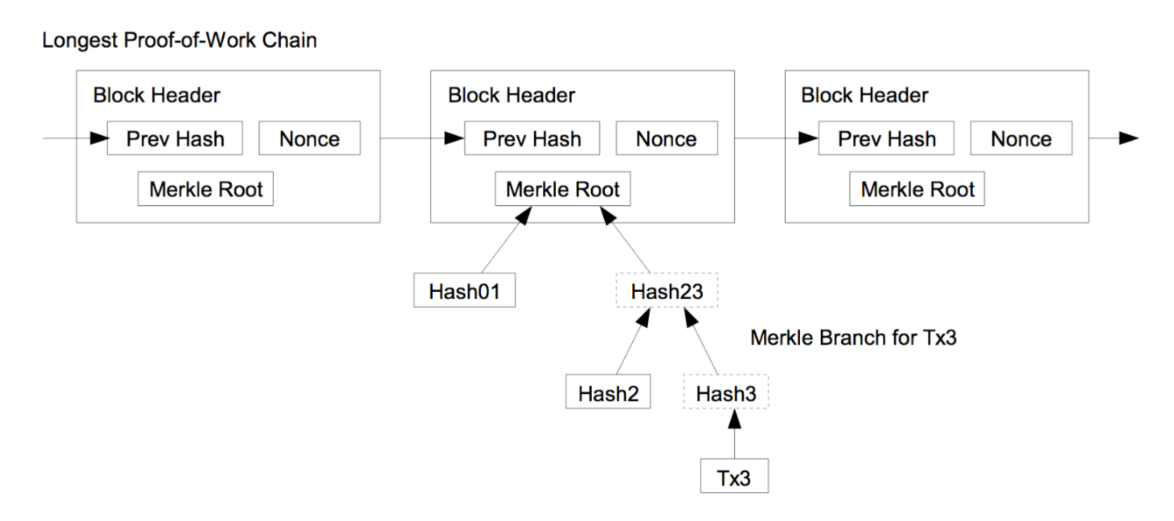


After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks a regenerated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it,and blocks added after it further confirm the network has accepted it.

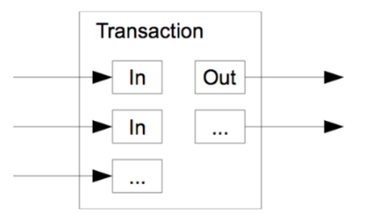


As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network

nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

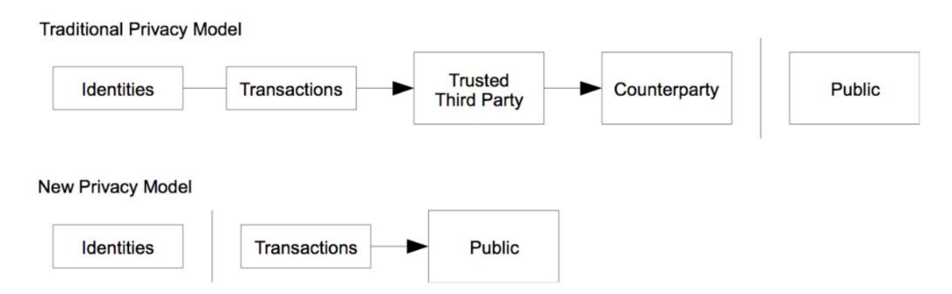
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publiclyprecludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sendingan amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the

same owner. The riskis that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing itslead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by **-**1.The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially aninfinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows **[8]**:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late. The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{Bmatrix} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{Bmatrix}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

q=0.1z=0

P=1.0000000z=1

P=0.2045873z=2

P=0.0509779z=3

P=0.0131722z=4

P=0.0034552z=5

P=0.0009137z=6

P=0.0002428z=7

P=0.0000647z=8

P=0.0000173z=9

P=0.0000046z=10

P=0.0000012q=0.3z=0

P=1.0000000z=5

P=0.1773523z=10

P=0.0416605z=15

P=0.0101008z=20

P=0.0024804z=25

P=0.0006132z=30

P=0.0001522z=35

P=0.0000379z=40

P=0.0000095z=45

P=0.0000024z=50

P=0.0000006

Solving for P less than 0.1%...

P < 0.001q=0.10

z=5q=0.15
z=8q=0.20
z=11q=0.25
z=15q=0.30
z=24q=0.35
z=41q=0.40
z=89q=0.45
z=340

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control ofownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodescontrol a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages arenot routed to any particular place and only need to be delivered on a best effort basis. Nodes canleave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance ofvalid blocks by working on extending them and rejecting invalid blocks by refusing to work onthem. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimaltrust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping,"In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

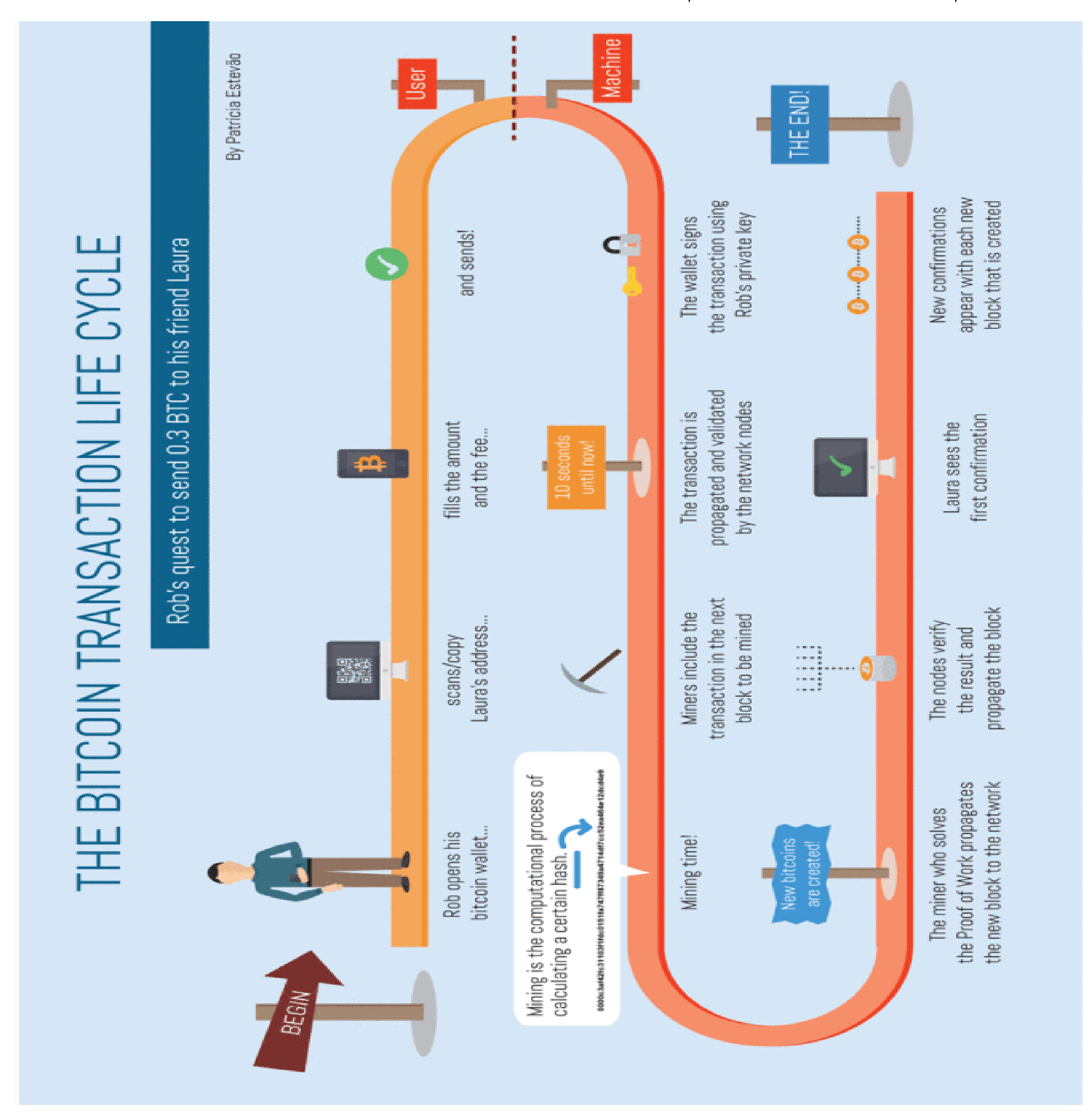
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conferenceon Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure,"http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security andPrivacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

ملحق رقم 2: آلية عمل نظام البيتكوين



مصوّر توضيحي: باتريسيا ايستيفاو

ملحق رقم 3: تحذير منشور من قبل قوى الأمن الداخلي اللبناني على مواقع التواصل الاجتماعي



منشور بتاريخ 18 نيسان 2020

ملحق رقم 4: إعلام رقم 900 – موجه للمصارف وللمؤسسات المالية ولمؤسسات الصرافة ولمؤسسات الوساطة المالية وللجمهور

19/Dec/2013

إعلام رقم 900

موجه للمصارف وللمؤسسات المالية

ولمؤسسات الصرافة ولمؤسسات الوساطة المالية وللجمهور

بالإشارة إلى القرار الأساسي رقم 7548 تاريخ 2000/3/30 المتعلق بالعمليات المالية والمصرفية بالوسائل الالكترونية لا سيما المادة 3 منه التي تحظر اصدار النقود الالكترونية (Electronic Money) من اي كان والتعامل بها بأي شكل من الاشكال،

ونظراً للمخاطر التي قد تنتج عن التعامل بالنقود الافتراضية بالأخص الـ Bitcoin ومنها:

1- ان المنصات (Platforms) أو الشبكات (Networks) التي يتم بواسطتها اصدار وتداول هذه النقود لا تخضع لأي تشريعات او تنظيمات وفي حال تعرضت لخسائر فلا يوجد اي اطار حماية قانوني يؤمن استرجاع الأموال التي تم بها شراء هذه النقود.

2- إن هذه النقود غير مصدرة أو مكفولة من أي مصرف مركزي وبالتالي فهي معرضة لتقلب حاد وسريع في أسعارها والتي يمكن أن تتدنى الى الصفر.

3- ان العمليات على النقود الافتراضية تسهّل استعمالها لنشاطات اجرامية خاصة لتبييض الأموال وتمويل الارهاب.

4- لا يمكن الرجوع عن العمليات أو التحاويل غير الصحيحة وغير الموافق عليها (Incorrect or Unauthorized) المنفذة بواسطة هذه النقود.

لذلك،

واستدراكاً للمخاطر والخسائر الجمة التي قد تنجم عن استعمال النقود الافتراضية،

فإن مصرف لبنان يحذر أي كان من شراء وحيازة واستعمال هكذا نقود.

بيروت في 19 كانون الأول 2013

حاكم مصرف لبنان

رياض توفيق سلامه

ملحق رقم 5: اعلام رقم 30 المتعلق بالمخاطر المتعلقة بالنقود الإلكترونية



إعلام رقم ٣٠

موجه الى المؤسسات المرخصة والجمهور
متعلق بالمخاطر المتعلقة بالنقود الإلكترونية

بناءً على القانون رقم ١٦١ تاريخ ٢٠١١/٨/١٧ المتعلق بالاسواق المالية،
وبناءً على قرار مجلس هيئة الاسواق المالية رقم ١٨/١/٧ المتخذ في جلسته المنعقدة بتاريخ ٢٠١٨/١/١٥،
وبناءً على قرار مجلس هيئة الاسواق المالية رقم ١٨/٢/٦ المتخذ في جلسته المنعقدة بتاريخ ٢٠١٨/٢/٥،

نحيطكم علماً بما يلي:

أولاً: يحظر على المؤسسات المرخصة إصدار النقود الإلكترونية (Electronic Money) كما يحظر عليها التسويق والتداول بالعملات الإلكترونية لحسابها أو لحساب عملائها بصورة مباشرة او غير مباشرة بما فيها المتداولة في الأسواق المالية المنظمة.

ثانياً: نظراً للمخاطر التي قد تنتج عن التعامل بالنقود الافتراضية بالأخص الـ Bitcoin ومنها ما يلي:

١- إن المنصّات (Platforms) أو الشبكات (Networks) التي يتم بواسطتها إصدار وتداول هذه النقود لا تخضع لأي تشريعات أو تنظيمات وفي حال تعرضت لخسائر فلا يوجد أي إطار حماية قانوني يؤمن استرجاع الأموال التي تم بها شراء هذه النقود.

٢- إن هذه النقود غير مصدرة أو مكفولة من أي مصرف مركزي وبالتالي فهي معرضة لتقلب حاد وسريع في أسعارها والتي يمكن أن تتدنى الى الصفر.

٣- إن العمليات على النقود الافتراضية تسهل استعمالها لنشاطات إجرامية خاصة لتبييض الأموال وتمويل الإرهاب.

٤- لا يمكن الرجوع عن العمليات أو التحاويل غير الصحيحة وغير الموافق عليها (Incorrect or Unauthorized) المنفذة بواسطة هذه النقود.

لذلك،

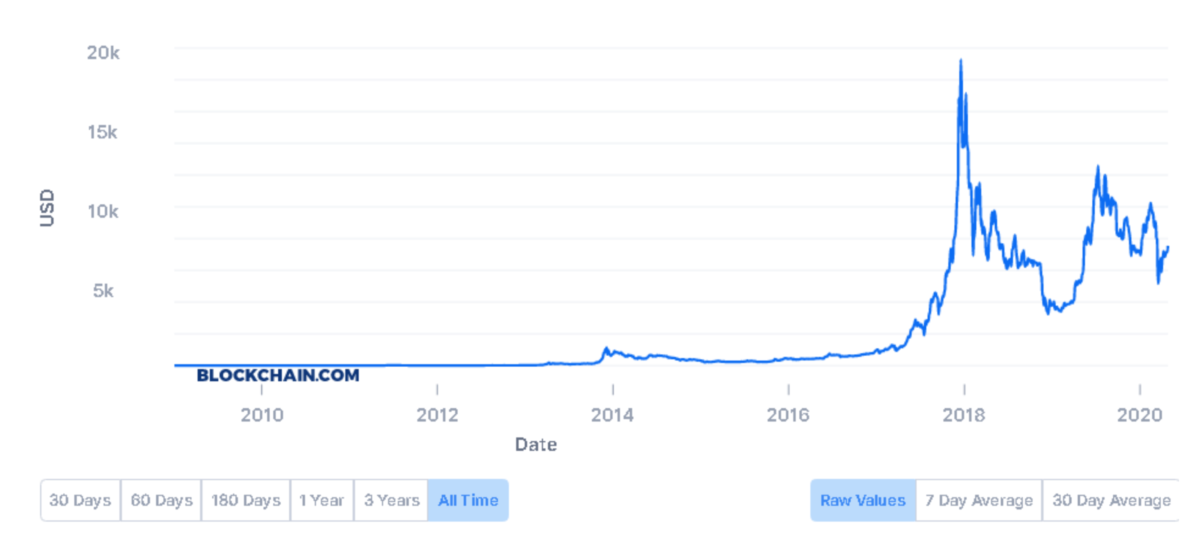
واستدراكاً للمخاطر والخسائر الجمة التي قد تنجم عن استعمال النقود الافترضية،
فإن هيئة الأسواق المالية تحذر أي كان من شراء وحيازة واستعمال هكذا نقود.

ثالثاً: يعمل بهذا الإعلام فور نشره في الجريدة الرسمية.

بيروت، في ١٢ شباط ٢٠١٨
رئيس هيئة الأسواق المالية/ حاكم مصرف لبنان
رياض توفيق سلامه

ملحق رقم 6: قيمة عملة البيتكوين على مدار السنين





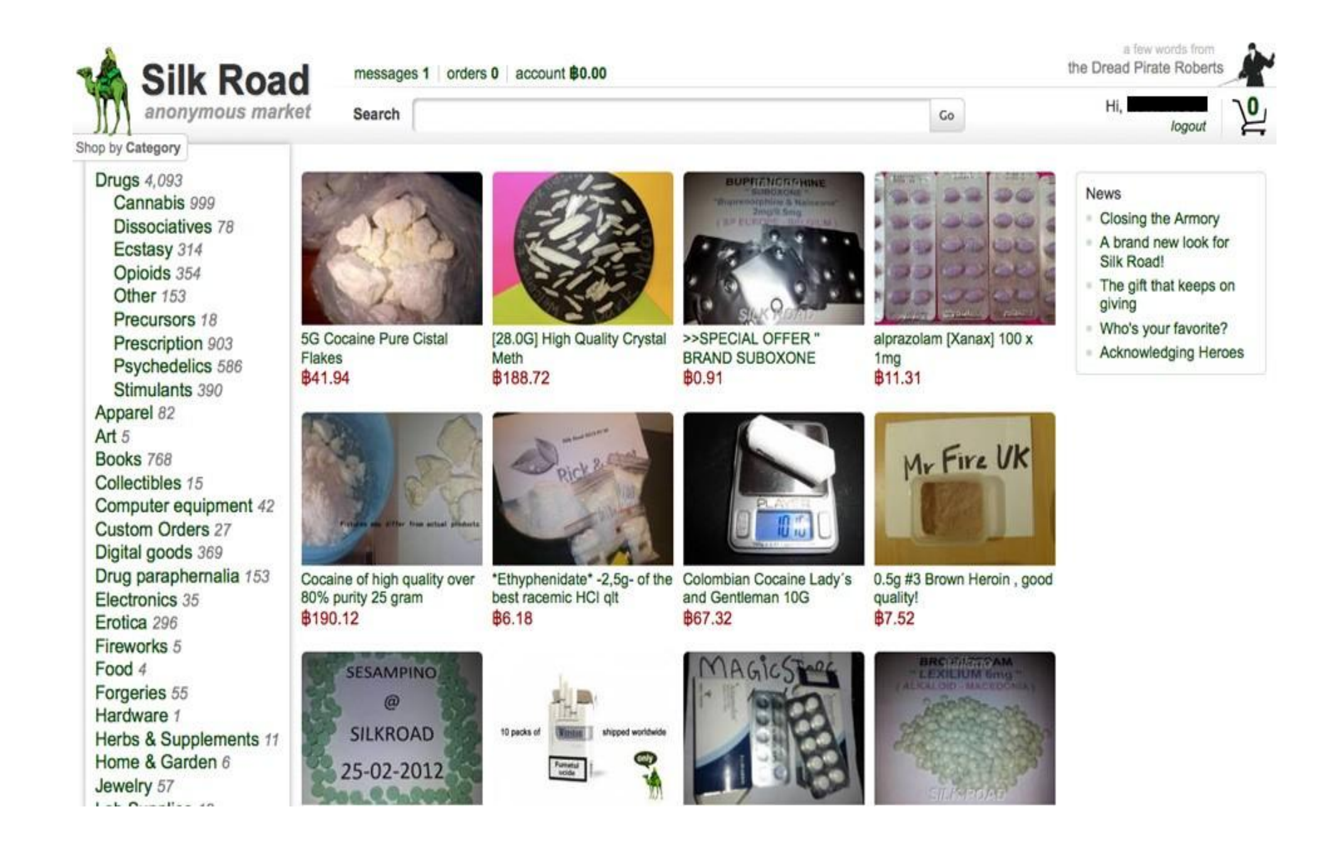
ملحق رقم 7: قائمة بأبرز العملات التشفيرية (مع القيمة السوقية)

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | Filters | USD ▾ | ← Back to Top 100

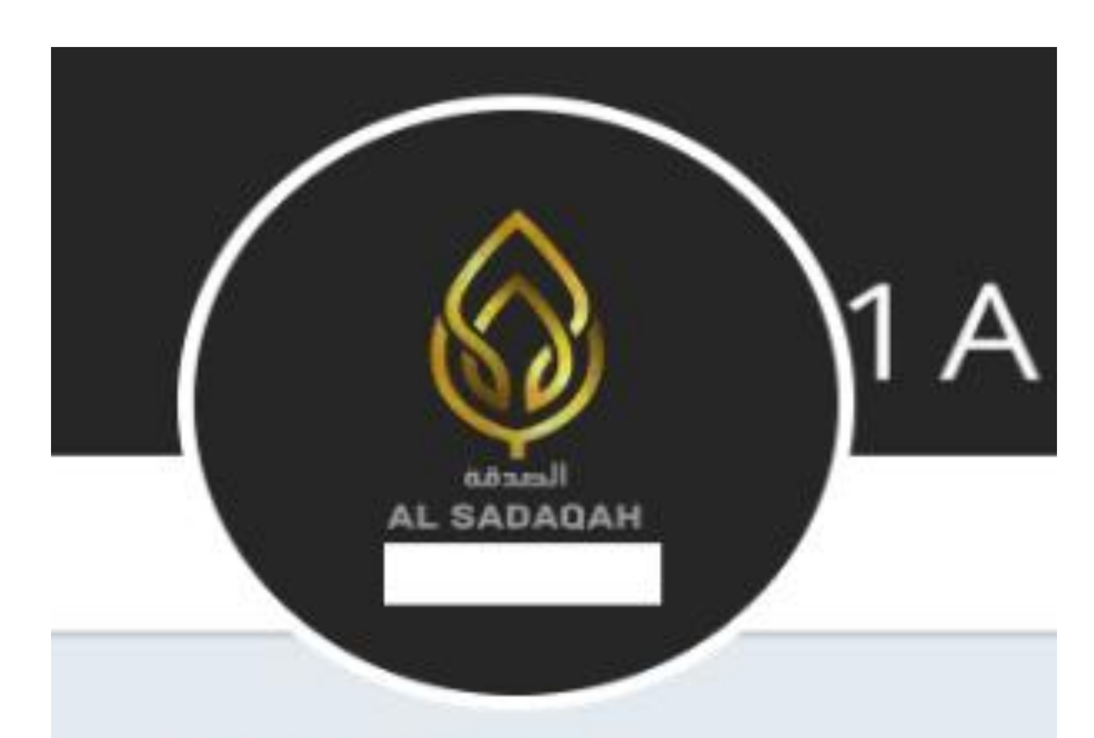
#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$153,578,907,002	$8,368.48	18,352,075 BTC	$45,740,039,977	0.39%	7.78%	18.33%
2	Ethereum	ETH	$23,353,122,343	$210.92	110,720,625 ETH	$22,620,894,220	0.31%	6.96%	16.84%
3	XRP	XRP	$9,795,738,117	$0.222061	44,112,853,111 XRP *	$2,783,405,191	0.37%	6.76%	18.20%
4	Bitcoin Cash	BCH	$4,651,698,624	$252.90	18,393,513 BCH	$4,099,238,004	0.37%	4.55%	9.76%
5	Bitcoin SV	BSV	$3,760,950,721	$204.49	18,391,958 BSV	$2,292,502,838	0.64%	5.41%	7.55%
6	Litecoin	LTC	$3,090,116,859	$47.82	64,618,931 LTC	$4,998,817,227	0.66%	6.64%	14.44%
7	EOS	EOS	$2,677,942,528	$2.90	922,202,124 EOS *	$4,606,062,592	0.51%	5.97%	11.53%
8	Binance Coin	BNB	$2,660,407,448	$17.10	155,536,713 BNB *	$418,129,034	0.45%	4.55%	9.52%
9	Tezos	XTZ	$2,013,006,234	$2.84	708,711,181 XTZ *	$285,633,368	0.22%	2.14%	24.02%
10	Stellar	XLM	$1,458,627,671	$0.071810	20,312,370,420 XLM *	$858,374,603	0.51%	4.37%	33.21%
11	Cardano	ADA	$1,317,088,070	$0.050800	25,927,070,538 ADA	$153,777,113	0.38%	7.53%	40.92%
12	Monero	XMR	$1,150,362,212	$65.58	17,541,408 XMR	$123,973,988	0.47%	4.96%	15.79%

المرجع: www.coinmarketcap.com تاريخ الزيارة 2020/4/29

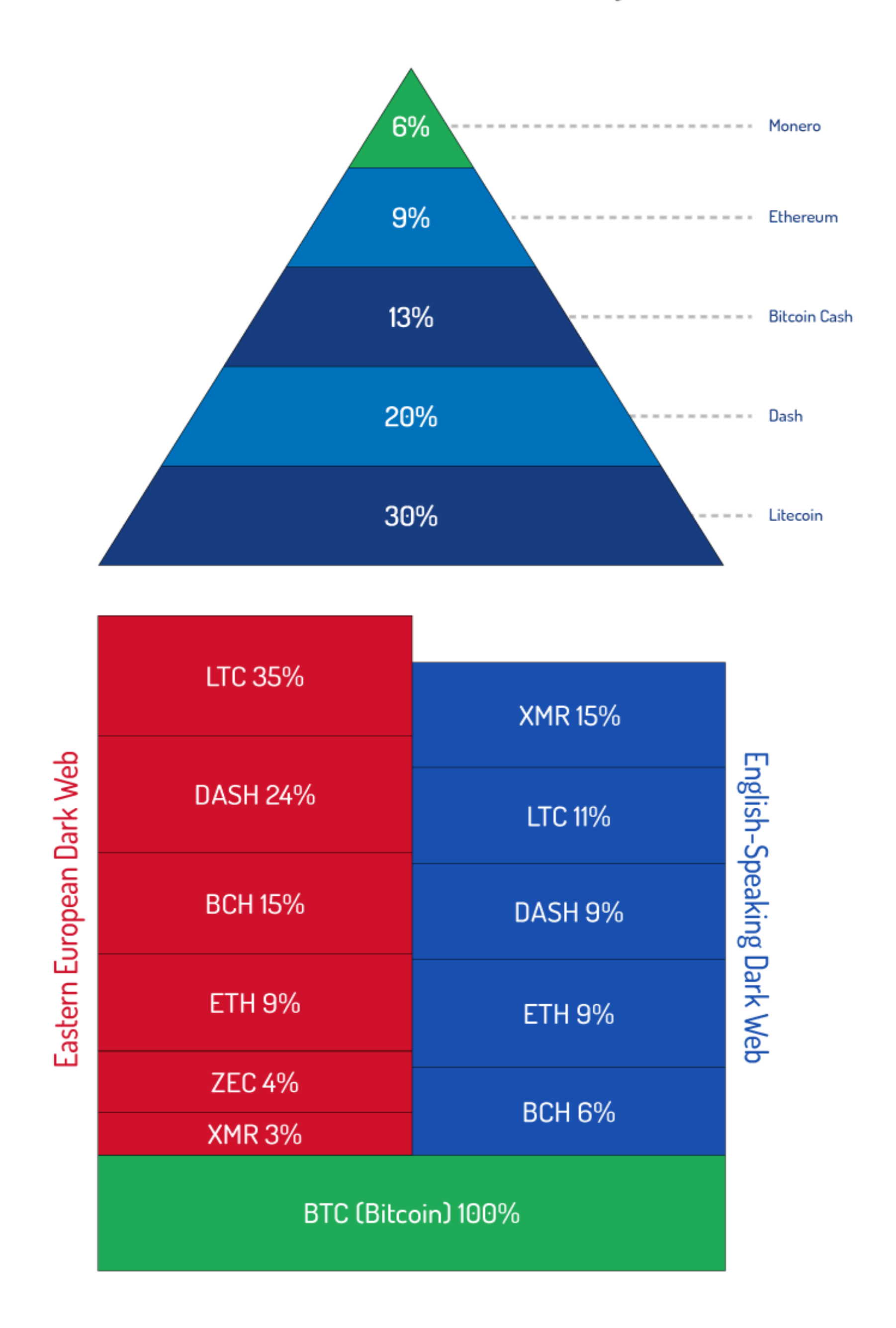
ملحق رقم 8: صورة لموقع SilkRoad



ملحق رقم 9: حساب تابع لمنظمة إرهابية (موقع تويتر)



ملحق رقم 10: العملات التشفيرية المستعملة على شبكة الإنترنت المظلم



المرجع: https://www.recordedfuture.com/

ملحق رقم 11: نموذج عن هجمة الرانسوم وير WannaCry



المرجع: موقع https://www.bbc.com/news

لائحة المراجع:

أولا: المراجع باللغة العربية

I. المؤلفات:

1. د. الحجار (وسيم)، **الاثبات الإلكتروني**، المنشورات الحقوقية صادر، 2007.
2. د. عالية (سمير)، وعالية (هيثم)، **القانون الجزائي للأعمال**، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الاولى، 2012.
3. د. عالية (سمير)، **الجرائم الواقعة على أمن الدّولة الخارجي والدّاخلي**، منشورات الحلبي الحقوقية، الطبعة الأولى، 2019.
4. د. الغول (حسين)، **جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها**، الطبعة الأولى، مكتبة بدران الحقوقية، 2017.

II. المؤلفات المعرّبة:

1. د. عمّوص (سيف الدّين)، **معيار البيتكوين البديل اللامركزي للنظام المصرفي المركزي**، ترجمة: محمد أحمد حمدان، الطبعة الأولى، تموز 2019.

III. الدراسات والمقالات:

1. أورديكيان (ماريلين)، "العملات الافتراضية المشفّرة في الحقل الجنائي السيبراني"، مجلة الدفاع الوطني، العدد 108، نيسان 2019، الصفحات 73-105، https://www.lebarmy.gov.lb/ar/content/108-d
2. شافي (نادر عبد العزيز)، " جرائم التزييف والتقليد والترويج النقدي"، مجلة الجيش، العدد 285، آذار 2009، https://www.lebarmy.gov.lb/ar/content/285-m%20

IV. الأطروحات والرسائل:

1. طوني عيسى، **التنظيم القانوني لشبكة الإنترنت دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية**، أطروحة أُعدت لنيل شهادة الدكتوراه، الجامعة اللبنانية كلية الحقوق والعلوم السياسية والإدارية الفرع الثاني، 2000.

V. النصوص القانونية:

- **اللبنانية:**

1. الدستور اللبناني، 1926.
2. قانون العقوبات اللبناني، 1943

3. قانون رقم 42 تاريخ 2015/11/24، الجريدة الرسمية، عدد 48 تاريخ 2015/11/26، الصفحات 3310-3312 (التصريح عن الأموال عبر الحدود).
4. قانون رقم 44 تاريخ 2015/11/24، الجريدة الرسمية، عدد 48 تاريخ 2015/11/26، الصفحات 3313-3318 (قانون مكافحة تبييض الأموال وتمويل الإرهاب).
5. قانون رقم 53 تاريخ 2015/11/24، الجريدة الرسمية، عدد 48 تاريخ 2015/11/26، (الإجازة للحكومة اللبنانية الانضمام إلى الاتفاقية الدولية لقمع تمويل الإرهاب الموقعة في نيويورك بتاريخ 1999/12/9).
6. قانون رقم 553 تاريخ 2003/10/20، الجريدة الرسمية، عدد 48 تاريخ 2003/10/22، ص. 188(إضافة مادة جديدة إلى قانون العقوبات).
7. قانون رقم 77 تاريخ 2016/10/27، الجريدة الرسمية، عدد 52 تاريخ 2016/11/3، الصفحات 3473-3474 (تعديل المادة 316 مكرر من قانون العقوبات).
8. قانون رقم 81 تاريخ 2018/10/10، الجريدة الرسمية، عدد 45 تاريخ 2018/10/18، الصفحات 4546-4568 (قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي).
9. القرار الأساسي رقم 12147 تاريخ 2015/12/22، الجريدة الرسمية، عدد 53 تاريخ 2015/12/31، الصفحات 3880-3879 (المتعلق بتطبيق قرارات مجلس الأمن رقم 1999/1267 ورقم 2011/1989 ورقم 2011/1988 والقرارات اللاحقة).
10. مصرف لبنان، اعلام رقم 900 تاريخ 19 كانون الأول 2013 موجه للمصارف وللمؤسسات المالية ولمؤسسات الصرافة ولمؤسسات الوساطة المالية وللجمهور، https://www.bdl.gov.lb/news/more/5/111/65
11. مصرف لبنان، قرار أساسي رقم 12836 تاريخ 2018/6/26، الجريدة الرسمية، عدد 30 تاريخ 2018/7/5 الصفحات 3981-3982 (المتعلق بمكافحة تبييض الأموال وتمويل الإرهاب).
12. هيئة الأسواق المالية، اعلام رقم 30 تاريخ 2018/2/12، الجريدة الرسمية، عدد 8 تاريخ 2018/2/22 (المخاطر المتعلقة بالنقود الإلكترونية).

- **العربية:**

13. قانون المالية الجزائري رقم 11-117، الجريدة الرسمية، عدد 76 تاريخ 28 كانون الأول 2017، https://www.joradp.dz/FTP/JO-ARABE/2017/A2017076.pdf

VI. الأحكام والقرارات القضائية:

1. محكمة التمييز الجزائية الغرفة السادسة، الرئيس رالف رياشي والأعضاء /عالية//سماحة/، قرار رقم 202 تاريخ 1997/12/23، منشور على موقع الجامعة اللبنانية مركز الأبحاث والدراسات في المعلوماتية القانونية، www.legiliban.ul.edu.lb

VII. المعاهدات والاتفاقيات الدولية:

1. الاتفاقية الدولية لقمع تمويل الإرهاب قرار رقم 109/54 لسنة 1999، www.treaties.un.org

VIII. وثائق الأمم المتحدة:

1. قرار الجمعية العامة رقم A/RES/71/291، الجلسة 71، 2017/6/19، www.un.org/en/ga/
2. قرار مجلس الأمن رقم 1373 تاريخ 28 أيلول 2001.
3. قرار مجلس الأمن رقم 2462 تاريخ 28 آذار 2019.

IX. المؤتمرات:

1. كلمة حاكم مصرف لبنان الأستاذ رياض سلامه خلال المؤتمر السابع لشركة سي.أس.آر. ليبانون **The 7th CSR Lebanon Forum**، في فندق فينيسيا، بيروت، 26 تشرين الأول 2017، http://www.bdl.gov.lb/news/more/8/250/251
2. كلمة حاكم مصرف لبنان الأستاذ رياض سلامه خلال ملتقى مكافحة الجريمة الإلكترونية الرابع **4th Anti-Cybercrime Forum**، في فندق فينيسيا، بيروت، 29 تشرين الثاني 2018.

X. المتفرقات:

1. مصرف البحرين المركزي، "مصرف البحرين المركزي يصدر التوجيهات النهائية الخاصة بخصوص الأصول المشفرة ومنصات الأصول المشفرة"، 25 شباط 2019، https://www.cbb.gov.bh/ar/media-center/
2. مكتب مكافحة الإرهاب-الأمم المتحدة فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب، "الصكوك الدولية لمكافحة الإرهاب"، الأمم المتحدة، https://www.un.org/counterterrorism/ctitf/ar/international-legal-instruments

ثانياً: المراجع باللغة الأجنبية

I. Books:

1. Ammous (Saifedean). **The Bitcoin Standard: The Decentralized Alternative to Central Banking**, John Wiley & Sons, 2018.
2. Antonopoulos (Andreas M.). **Mastering Bitcoin: Programming The Open Blockchain**, "O'Reilly Media, Inc.", 2nd edition, 2017.
3. Casey (Eoghan). **Digital Evidence and Computer Crime: Forensic Science, Computers, And The Internet**, Academic press, 2011.
4. Casey (Michael J.), Vigna (Paul). **The Truth Machine: The Blockchain and the Future of Everything**, St. Martin's Press, New York, February 2018.
5. Eha (Brian Patrick). **How Money Got Free: Bitcoin and the Fight for the Future of Finance**, Oneworld Publications, 2017.
6. Narayanan (Arvind), et al. **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**, Princeton University Press, 2016.
7. Rosario (Girasa). **Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives**, Springer, 2018.
8. Vigna (Paul), Casey (Michael J.). **The Age of Cryptocurrency: How Bitcoin and The Blockchain are Challenging The Global Economic Order**, Picador, 2016.

II. Articles:

1. Abrar (Waleed). "Untraceable electronic cash with Digicash," University of Konstanz, Jul. 2014.
2. Ammous (Saifedean). "Can Bitcoin's Volatility Be Tamed?", The Journal of Structured Finance, Vol. 24.1, 2018, pp. 53-60.
3. Angel (James J.), McCabe (Douglas). "The ethics of payments: Paper, plastic, or bitcoin?" Journal of Business Ethics, Vol. 132.3, 2015, pp. 603-611.

4. Beshiri (Arbër S.), Susuri (Arsim). "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review." Journal of Computer and Communications, Vol. 7.3, 2019, pp. 30-43.
5. Bischoping (Gregory). "Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016." University of Pennsylvania Law Review, Vol. 167, 2018, pp. 239-259.
6. Bollen (Rhys). "The legal status of online currencies: are Bitcoins the future?", Journal of Banking and Finance Law and Practice, Vol. 24.4, December 2013.
7. Bouveret (Antoine), Haksar (Vikram). "What Are Cryptocurrencies? A Potential New Form of Money Offers Benefits While PosingRisks," **Money, Transformed The Future of Currency in a Digital World**, International Monetary Fund, June 2018.
8. Brown (Steven David). "Cryptocurrency and Criminality: The Bitcoin Opportunity." The Police Journal, Vol. 89.4, Dec. 2016, pp. 327–339.
9. Chaum (David). "Blind signatures for untraceable payments." Advances in cryptology*, Springer*, 1983, pp. 199-203.
10. Chui (Michael KF), et al. "The collapse of international bank finance during the crisis: evidence from syndicated loan markets." BIS Quarterly Review, Sept. 2010, pp. 39-49.
11. Conti (Mauro), et al. "A Survey on Security and Privacy Issues of Bitcoin." IEEE Communications Surveys & Tutorials, Vol. 20.4, 2018, pp. 3416-3452.
12. Goldsborough (Reid). "The Lydian Lion: a case for the world's first coin." The Journal of the Classical & Medieval Numismatic Society, Series Two, Vol. 5.3, September 2004, pp. 111-125.
13. Gordon (Sarah), Ford (Richard). "On the definition and classification of cybercrime." Journal in Computer Virology, Vol. 2.1, 2006, pp. 13-20.
14. Gross (Michael L.), et al. "The psychological effects of cyber terrorism." Bulletin of the Atomic Scientists, Vol. 72.5, 2016, pp. 284-291.

15. Li (Jiasun), Mann (William). "Initial Coin Offerings and Platform Building," 2018 WFA, 2019 AFA.
16. Narayanan (Arvind). "What Happened to the Crypto Dream?, Part 1," IEEE Security & Privacy, Vol. 11.2, March–April 2013, pp. 75-76.
17. Realuyo (Celina). "North American Effort to Combat the Financing of Terrorism." **SOF Role in Combating Transnational Organized Crime**, The JSOU Press MacDill Air Force Base, Florida, 2016, pp. 85-108.
18. Reynolds (Perri), Irwin (Angela SM). "Tracking Digital Footprints: Anonymity within The Bitcoin System." Journal of Money Laundering Control, Vol. 20.2, 2017. pp. 172-189.
19. Salami (Iwa). "Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?", Studies in Conflict & Terrorism, Vol. 41.12, 2018, pp. 968-989.
20. Stratiev (Oleg). "Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand." Banking & Finance Law Review, Vol. 33.2, 2018, pp. 173-212.
21. Trautman (Lawrence J.). "Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?" Richmond Journal of Law and Technology, Vol. 20.4, 2014, pp. 1-108.
22. Turpin (Jonathan B.). "Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework." Indiana Journal of Global Legal Studies, Vol. 21, 2014, pp. 335-368.

III. Studies:

1. Claeys (Grégory), et al. Study requested by the European Parliament's Economic and Monetary Affairs Committee (ECON), on "**Cryptocurrencies and Monetary Policy**," No. PE 619.018, Jun. 2018.
2. Fiedler (Salomon), et al. Study requested by the European Parliament's Economic and Monetary Affairs Committee (ECON), on "**Virtual Currencies**," No. PE 619.016, Brussels, 2018.

3. Finck (Michèle). Study requested by the European Parliament's the Panel for the Future of Science and Technology (STOA), on "**Blockchain and The General Data Protection Regulation: Can Distributed Ledgers Be Squared With European Data Protection Law?**" No. PE 634.445, Brussels, July 2019.
4. Houben (Robby), Snyers (Alexander). Study requested by the European Parliament's TAX3 Committee, on "**Cryptocurrencies and Blockchain Legal Context and Implications for Financial-Crime, Money Laundering and Tax Evasion**," No. PE 619.024, Brussels, July 2018, http://www.europarl.europa.eu/committees/en/supporting-analyses-search.html
5. Keatinge (Tom), et al. Study commissioned by European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, on "**Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses: Counter-terrorism**," No. PE 604.970, May 2018.

IV. Reports and Papers:

1. Baran (Paul). Report **On distributed communications: I. Introduction to distributed communications networks**, United States Air Force Project RAND, RM-3420-PR, 1964.
2. Chainalysis. Report on **The 2020 State of Crypto Crime**, January 2020, www.chainalysis.com
3. Chiu (Jonathan), Koeppl (Thorsten V.). Paper on **Incentive compatibility on the blockchain**, Bank of Canada, No. 2018-34, July 2018, https://www.bankofcanada.ca
4. Cyber Threat Alliance. Report on **The Illicit Cryptocurrency Mining Threat**, September 2018, https://www.cyberthreatalliance.org/resources/

5. European Central Bank Crypto-Assets Task Force. Paper on **Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures**, No. 223, May 2019, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf
6. Europol. Report on **Internet Organised Crime Threat Assessment**, Doi 10.2813/858843, 2018, www.europol.europa.eu.
7. Fanusie (Yaya), Enetz (Alex). Report on **Al-Qaeda in the Islamic Maghreb Financial Assessment**, Center on Sanctions & Illicit Finance, 2017, https://www.fdd.org/analysis/2017/12/07/terror-finance-briefing-book/
8. FATF. Report on **Emerging Terrorist Financing Risks**, Paris, 2015, http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.
9. FATF. Report on **Virtual Currencies Key Definitions and Potential AML/CFT Risks**, France, June 2014, http://www.fatf-gafi.org/publications
10. Griffoli (Tommaso Mancini), et al. Paper on **Casting Light on Central Bank Digital Currencies**, International Monetary Fund, SDNEA2018008, 12 Nov. 2018, https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233
11. Jenik (Ivo), Lauer (Kate). Working paper on "Regulatory sandboxes and financial inclusion." Washington, DC: CGAP, 2017.
12. Kaspersky Lab. Annual report on **Ransomware and Malicious Cryptominers 2016-2018**, 27 Jun. 2018, www.securelist.com
13. Office Parlementaire d'évaluation des Choix Scientifiques et Technologiques, **Rapport sur les enjeux technologiques des blockchains (chaînes de blocs)**, 4 Juin 2018, https://www.senat.fr/rap/r17-584/r17-5841.pdf

14. Rapport au Ministre de l'Economie et des Finances, **Les crypto-monnaies**, 4 Juillet 2018, https://www.mindfintech.fr/files/documents/Etudes/Landau_rapport_cryptomonnaies_2018.pdf
15. Symantec. Annual Report on **The evolution of ransomware**, Version 1.0, 6 Aug. 2015, www.symantec.com
16. Symantec. Internet Security Threat Report on **Cryptojacking: A Modern Cash Cow**, September 2018, www.symantec.com

V. Theses and Dissertations:

1. Baum (Stafford C.). **Cryptocurrency Fraud: A Look into the Frontier of Fraud**, *University Honors Program Theses*, 2018, https://digitalcommons.georgiasouthern.edu/honors-theses/375
2. Bray (Jesse D.). **Anonymity, Cybercrime, and the Connection to Cryptocurrency**, master's thesis, *Eastern Kentucky University*, 2016, https://encompass.eku.edu/etd/344

VI. Laws, Regulations and Legal Texts:

Canada:

1. Bill C-31, An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures, Second Session, Forty-first Parliament, 62-63 Elizabeth II, 2013-2014, Statutes of Canada 2014 Ch. 20, https://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/third-reading
2. Canadian Currency Act, R.S.C., 1985, https://laws-lois.justice.gc.ca/eng/acts/c-52/FullText.html
3. Financial Consumer Agency of Canada. **"Digital Currency," 2018**, https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html#toc0

4. Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019: SOR/2019-240, Canada Gazette, Part II, Volume 153, Number 14, 10 July 2019.

Estonia:

5. Estonian "Money Laundering and Terrorist Financing Prevention Act" of 27 Nov. 2017.

France:

6. Décret No. 2019-1213 du 21 Novembre 2019 relatif aux prestataires de services sur actifs numériques, JORF No. 0271 du 22 Novembre 2019, texte No. 25.
7. LOI no. 2019-486 du 22 Mai 2019 relative à la croissance et la transformation des entreprises (1), JORF No. 0119 du 23 Mai 2019, texte No. 2.
8. Règlement général de l'Autorité des marchés financiers, ELI: /eli/fr/aai/amf/rg/livre/2/titre/3/chapitre/1/section/7/20191219/notes/fr.html

Germany:

9. BaFin. "Virtual Currency (VC)," Federal Financial Supervisory Authority, https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html
10. German Federal Ministry of Finance (BMF). "VAT Treatment of Bitcoin and Other So-Called Virtual Currencies-ECJ Decision of October 2015, C-264/14, Hedqvist (BMF Letter)," 27 Feb. 2018, https://www.loc.gov/law/foreign-news/article/germany-federal-ministry-of-finance-publishes-guidance-on-vat-treatment-of-virtual-currencies/

United States of America:

11. FinCen. “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies”, FIN-2019-G001, 9 May 2019, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models

12. Securities and Exchange Commission. "Pump and Dump Schemes," March 2001, https://www.sec.gov/fast-answers/answerspumpdumphtm.html

VII. European Directives:

1. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, **Official Journal of the European Union**, L.267/7, 10 Oct. 2009.
2. Directive 843/2018 of the European Parliament and of the Council of 30 May 2018 amending Directive 849/2018 on the prevention of the use of financial system for the purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, **Official Journal of the European Union**, L.156, 19 Jun. 2018.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation), **Official Journal of the European Union**, L.119/1, 4 May 2016.

VIII. International and Regional Legal Texts:

1. European Central Bank. “Virtual Currency Schemes,” October 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

2. European Central Bank. “Virtual Currency Schemes,” February 2015, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
3. FATF. “Guidance for a Risk Based Approach: Virtual Currencies,” France, June 2015, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
4. FATF. “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
5. FATF. “International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation-The FATF Recommendations,” June 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/
6. FATF. “Regulation of Virtual Assets,” France, 19 Oct. 2018, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/regulation-virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)
7. The European Securities and Markets Authority-ESMA. Statement: "ESMA Highlights ICO Risks for Investors and Firms,” 13 Nov. 2018, https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms

IX. Cases:

1. *Bitconnect Securities Litigation, Wildes et al. v. BitConnect Trading Ltd. et al.*, No.9:2018cv80086.
2. U.S. Attorney's Office of Southern District of New York, *Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts,* 5 Feb. 2015, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts

3. U.S. District Court Judge in Eastern District of Virginia, *Virginia Teen Pleads Guilty to Providing Material Support to ISIL*, Press release No. 15-727, 11 Jun. 2015, https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil
4. U.S. Federal Court in Central Islip New York, *Long Island Woman Pleads Guilty to Providing Material Support to ISIS*, Docket No. 17-CR-690 (JS), 26 Nov. 2018. https://www.justice.gov/usao-edny/pr/long-island-woman-pleads-guilty-providing-material-support-isis
5. U.S. Securities and Exchange Commission v. PlexCorps, Dominic Lacroix, and Sabrina Paradis-Royer, No. 1:17-cv-07007-CBA-RML (E.D.N.Y. 2 Oct. 2019)
6. U.S. The Securities and Exchange Commission, *SEC Charges Issuer With Conducting $100 Million Unregistered ICO*, 4 Jun. 2019, https://www.sec.gov/news/press-release/2019-87
7. U.S. The Securities and Exchange Commission, *SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds*, 29 Sept. 2017, https://www.sec.gov/news/press-release/2017-185-0
8. *United States v. Liberty Reserve*, 13 Crim. 368 (S.D.N.Y. May 20, 2013).

X. Website Articles:

1. “La gendarmerie a neutralisé un réseau de 850 000 ordinateurs infectés par le même virus,” Le Monde, 28 Aug. 2019, https://www.lemonde.fr/pixels/article/2019/08/28/la-gendarmerie-a-neutralise-un-reseau-de-850-000-ordinateurs-infectes-par-le-meme-virus_5503771_4408996.html
2. “Man acquitted over cryptomining program that used site visitors' PCs.” Japan Today, 28 Mar. 2019, https://japantoday.com/category/crime/man-acquitted-over-cryptomining-program-that-used-site-visitors'-pcs

3. Alexander (Doug). "Crypto CEO Holding Only Passwords That Can Unlock Millions in Customer Coins," Bloomberg, 4 Feb. 2019, https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem
4. Alford (Tom). "Bitconnect Scam: The $2.6 BN Ponzi Scheme [2019 Update]," TotalCrypto.io, 8 Oct. 2018, https://totalcrypto.io/bitconnect-scam/
5. Al-Shikarchy (Mariam), et al. "Canadian Taxation of Cryptocurrency ... So Far," Gowling WLG, *Lexology*, 14 Nov. 2017, https://www.lexology.com/library/
6. Anderson (Brooke) . "Salameh: Central Bank to Launch Digital Currency," The Daily Star, 27 Oct. 2017, https://www.dailystar.com.lb/Business/Local/2017/Oct-27/424064-salameh-central-bank-to-launch-digital-currency.ashx
7. Aro.steem. "Lebanese Crypto-currencies Stolen Users-sms Attack," steempeak.com, November 2019, https://steempeak.com/@aro.steem/crypto-stolen-users-lebanese-telecom-touch-ss7-firewall-has-been-breached?fbclid=iwar1eddn4jei3ynpta56lfkz0pw3l0gnh4a_e9jueg41qdmbomvvp6kk2ywm
8. Avan-Nomayo (Osato). "51 Percent: Hackers Steal $18 Million In Bitcoin Gold (BTG) Tokens." Bitcoinist.com, 26 May 2018, https://bitcoinist.com/51-percent-attack-hackers-steals-18-million-bitcoin-gold-btg-tokens/
9. Azhari (Timour). "Distrust in Lebanese banks spurs bitcoin boom." Al Jazeera, 25 Feb. 2020, www.aljazeera.com
10. Baranetsky (Victoria). "What is cyberterrorism? Even experts can't agree," The Harvard Law Record, 5 Nov. 2009, https://web.archive.org/web/20091112093639/http://www.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186

11. Barrier (Eric) . “Lebanese central bank issues Middle East’s first Bitcoin warning,” Cointelegraph, 3 Jan. 2014, https://cointelegraph.com/news/lebanese_central_bank_issues_middle_east_s_first_bitcoin_warning
12. BBC News. “Coincheck: World's biggest ever digital currency 'theft',” bbc.com, 27 Jan. 2018, https://www.bbc.com/news/world-asia-42845505
13. Bender (Ruth), Alessi (Christopher). “Munich Shooter Likely Bought Reactivated Pistol on Dark Net.” The Wall Street Journal, 24 Jul. 2016, https://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686
14. Brustein (Joshua). “Bitcoin May Not Be So Anonymous, After All.” Bloomberg, 27 Aug. 2013, www.bloomberg.com/news/articles/2013-08-27/bitcoin-may-not-be-so-anonymous-after-all
15. Cartwright (Mark). “Ancient Greek Coinage.” Ancient History Encyclopedia, 15 Jul. 2016, www.ancient.eu/Greek_Coinage/
16. Cavicchioli (Marco). “What Is and How Double-Spending Works? - NovaMining Media.” Medium, *NovaMining Media*, 4 Jul. 2018, medium.com/novamining/what-is-and-how-double-spending-works-ee45e6433910
17. CB Insights. “Blockchain Startups Absorbed 5X More Capital Via ICOs Than Equity Financings In 2017,” cbinsights.com, 18 Jan. 2018, https://www.cbinsights.com/research/?s=Blockchain+Startups+Absorbed+5X+More+Capital+Via+ICOs+Than+Equity+Financings+In+2017
18. Chabrow (Eric). “Can Cyber Terrorism Exist? - Interview with Jim Harper of the Cato Institute,” Government Info Security News, 10 Jul. 2009, https://www.govinfosecurity.com/interviews/cyber-terrorism-exist-interview-jim-harper-cato-institute-i-283

19. Cuthbertson (Anthony). “#OpParis: Anonymous pursuit of Isis sees jihadists retreat to the dark web.” International Business Times, 18 Nov. 2015, https://www.ibtimes.co.uk/isis-moves-dark-web-escape-anonymous-opparis-1529351
20. Duhaime (Christine). “Canada Implements World’s First National Bitcoin Law,” DUHAIME LAW, 22 Jun. 2014, https://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/
21. Emerging Technology from the arXiv. “True Scale of Bitcoin Ransomware Extortion Revealed.” MIT Technology Review, 19 Apr. 2018, www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/
22. Fanusie (Yaya). “Terrorist Networks Eye Bitcoin as Cryptocurrency’s Price Rises,” The Cipher Brief (blog), 21 Dec. 2017, https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises
23. Goldman (Russell). “What We Know and Don't Know About the International Cyberattack.” The New York Times, 12 May 2017, www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html
24. Helms (Kevin). “Japan Gives Jail Sentence to Crypto Miner in a Remote Mining Case.” Bitcoin News, 3 Jul. 2018, news.bitcoin.com/japan-jail-sentence-crypto-miner-remote-mining/
25. Japan court convicts man of installing cryptomining programs without consent,” The Mainici, 7 Feb. 2020, https://mainichi.jp/english/articles/20200207/p2g/00m/0dm/083000c
26. Kafeine. “Smominru Monero mining botnet making millions for operators.” ProofPoint, 31 Jan. 2018, https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

27. Katalyse.io. "How Cryptocurrency is Disrupting the Global Economy," Medium, 10 Jan. 2018, https://medium.com/the-mission/how-cryptocurrency-is-disrupting-the-global-economy-89347581aa93
28. Kelly (Jemima), Wilkes (Tommy). "Exclusive: Coincheck Hackers Trying to Move Stolen Cryptocurrency-Executive," Reuters, 30 Jan. 2018, https://www.reuters.com/article/us-japan-cryptocurrency-cybercrime/exclusive-coincheck-hackers-trying-to-move-stolen-cryptocurrency-executive-idUSKBN1FJ28Y
29. Kharpal (Arjun). "Tokenization: The World of ICO's," CNBC, 16 Jul. 2018, https://www.cnbc.com/2018/07/13/initial-coin-offering-ico-what-are-they-how-do-they-work.html
30. Malik (Nikita). "How The Darknet Can Be Used By Terrorists To Obtain Weapons." Forbes, 15 Jan. 2019, https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/
31. Manheim (David), et al., "Are Terrorists Using Cryptocurrencies?" Foreign Affairs, 21 Apr. 2017, https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies
32. *Manning (Landon). "I*MF and World Bank Launch 'Learning Coin' to Explore Cryptocurrency," Nasdaq, 15 May 2019, https://www.nasdaq.com/articles/imf-and-world-bank-launch-learning-coin-explore-cryptocurrency-2019-05-15
33. Moos (Mitchell). "Analysis: Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco." CryptoSlate, 29 Nov. 2018, cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/
34. Nadeem (Maher). "Some see Bitcoin as haven in crisis-hit Lebanon." The Daily Star, 31 Jan. 2020, www.dailystar.com.lb

35. Pinkstone (Joe). "RobinHood Ransomware Attack That Paralysed Baltimore's Government Could Be Coming to YOUR City." Daily Mail Online, Associated Newspapers, 29 May 2019, www.dailymail.co.uk/sciencetech/article-7082001/RobinHood-ransomware-attack-paralysed-Baltimores-government-coming-city.html
36. Redman (Jamie). "When It Comes to Scarcity and Anti-Counterfeiting Bitcoin Actually Outshines Gold." Bitcoin News, 11 Apr. 2017, news.bitcoin.com/scarcity-anti-counterfeiting-bitcoin-outshines-gold/
37. Salmon (Felix). "The Bitcoin Bubble and the Future of Currency," Medium, 3 Apr. 2013, https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb
38. Schulze (Elizabeth). "Cryptocurrencies are 'clearly shaking the system,' IMF's Lagarde says," CNBC, 10 Apr. 2019, https://www.cnbc.com/2019/04/11/cryptocurrencies-fintech-clearly-shaking-the-system-imfs-lagarde.html
39. Serres (Tom). "2017's Ransomware Attacks: Could Blockchain Technology Have Prevented Them?", Medium, 30 May 2017, medium.com/animal-meia/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b
40. Simone (Alina). "The Strange History of Ransomware." Medium, 26 Mar. 2015, medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b
41. Smith (Graham). "Lebanon Fights for Separation of Money and State as Residents Use Bitcoin to Evade Capital Control." Bitcoin.com, 27 Feb. 2020, www.news.bitcoin.com
42. Suberg (William). "Bitcoin Exchange ShapeShift Helps Police as WannaCry Attacker Converts to Monero." Cointelegraph, 4 Aug. 2017, cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero

43. Symantec. "What is cryptojacking? How it works and how to help prevent it." Norton, https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html
44. Taylor (Adam). "The Islamic State (or someone pretending to be it) Is Trying To Raise Funds Using Bitcoin." The Washington Post, 9 Jun. 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin/?noredirect=on&utm_term=.c7404e464ffb
45. Team InnerQuest Online. "How Does a Blockchain Prevent Double-Spending of Bitcoins?" Medium, *InnerQuest Online*, 25 Aug. 2018, medium.com/innerquest-online/how-does-a-blockchain-prevent-double-spending-of-bitcoins-fa0ecf9849f7
46. Yakubowski (Max). "Bank of Canada Study Finds Double Spending in Blockchain is 'Unrealistic'." CoinTeleghraph, 22 Jul. 2018, https://cointelegraph.com/news/bank-of-canada-study-finds-double-spending-in-blockchain-is-unrealistic

XI. Conference Papers:

1. Biryukov (Alex), et al. "Deanonymisation of clients in Bitcoin P2P network." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2014.
2. Kabay (Michel E.). "Anonymity and pseudonymity in cyberspace: deindividuation, incivility and lawlessness versus freedom and privacy." *Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR)*, Vol. 16, 1998, p. 14. http://www.mekabay.com/overviews/anonpseudo.pdf
3. Meiklejohn (Sarah), et al. "A fistful of bitcoins: characterizing payments among men with no names," *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 127-140.

4. O'Loughlin (Erin K.), Lormel (Dennis). "Terror Finance And Technology", *Bank of America*, West Coast AML Forum 2015 May 6-8, 2015.
5. Pastrana (Sergio), Suarez-Tangil (Guillermo). "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth." *Proceedings of the Internet Measurement Conference*, 2019, pp. 73-86.

XII. Miscellaneous:

1. Lagarde (Christine). "Winds of Change: The Case for New Digital Currency," International Monetary Fund, 14 Nov. 2018, https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency
2. Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/en/
3. U.S. SEC. "Framework for "Investment Contract "Analysis of Digital Assets," 3 Apr. 2019, https://www.sec.gov/files/dlt-framework.pdf
4. Wei Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

XIII.Websites:

https://archive.org/
https://bitcoinfees.earn.com/
https://coinatmradar.com/
https://coinmarketcap.com/
https://cs.stanford.edu/
https://eur-lex.europa.eu/homepage.html?locale=en
https://satoshi.nakamotoinstitute.org/emails/cryptography/1/
http://securities.stanford.edu/
https://ssrn.com/
https://twitter.com/
https://www.binance.com/en

https://bitcoin.org/en/
https://www.blockchain.com/
https://www.coinbase.com/
https://www.crypto51.app/
https://www.ecb.europa.eu/
https://www.fatf-gafi.org/
https://www.imf.org/
https://www.kraken.com/
http://www.legallaw.ul.edu.lb/
https://www.legifrance.gouv.fr/
https://www.rain.bh/
https://www.recordedfuture.com/
https://www.reddit.com/
https://www.researchgate.net/
https://www.sec.gov/
https://www.statista.com/
https://twitter.com/
https://www.un.org/en/

الفهرست